VŠB - Technická univerzita Ostrava

Fakulta elektrotechniky a informatiky

Katedra telekomunikační techniky

Využití biometrie pro bezpečné přihlašování do sítí

Using biometric for security access to networks

2009 Zdeněk Doložílek

Prohlášení

Prohlašuji, že jsem tuto diplomovou práci vypracoval samostatně. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

V Ostravě dne: …… ……

podpis

Poděkování

Chtěl bych poděkovat panu Ing. Pavlu Nevludovi za jeho vstřícný přístup a odbornou pomoc při psaní této diplomové práce.

Abstrakt

Diplomová práce se zabývá problematikou biometrie. V první časti popisuje teoretický rozbor obecných vlastností biometrie, různé druhy biometrických metod a síťové protokoly.

V druhé části je řešena praktická problematika návrhu pracoviště pro snímání vzorku otisku prstů. Je zde uveden popis zvolené čtečky, instalace potřebného softwaru a jeho nastavení.

Závěrečná část je pojata jako grafická prezentace řešené problematiky, od samotné instalace potřebných komponent až po vlastní přihlášení do sítě.

Klíčová slova

Identifikace, verifikace, srovnávání, biometrický vzorek, markanty, protokol, čtečka otisku prstů, snímače, Linux

Abstract

Thesis deals with biometrics. The first part describes the theoretical analysis of the general characteristics of biometrics, the different types of biometric methods and network protocols.

The second part is dealt with practical issues of workstation proposal for scanning a sample fingerprint. There is a description of the selected reader, install the necessary software and setup.

The final part is designed as a graphical presentation of tackle, from the very necessary installation components to your own login to the network.

Key words

Identification, verification, matching, biometric sample, markant, protocol, reader fingerprint, sensor, Linux

Seznam použitých symbolů a zkratek

ARP	– Address Resolution Protocol
CMOS	– Complementary Metal–Oxide–Semiconductor
DHCP	– Dynamic Host Configuration Protocol
DNS	– Domain Name System
EBGM	– Elastic bunch graph matching
EER	– Equal Error Rate
FAR	– False Acceptance Rate
FIR	– False Identification Rate
FRR	– False Rejction Rate
FTA	– Failure To Acquire rate
FTE	– Failure To Enroll rate
ICMP	– Internet Control Message Protocol
IPv4	– Internet protokol verze 4
IPv6	– Internet protokol verze 6
LED	– Light-Emitting Diode
PDA	– Personal digital assistant
SW	– Software
TCP/IP	– Transmission Control Protocol/ Internet Protocol
UDP	– User Datagram Protocol

Obsah

1 Úvod

Pro bezpečné přihlašování do sítě se v poslední době čím dál více využívá biometrických metod. Biometrické metody jsou založeny na rozpoznávání fyzických charakteristik člověka. Tyto metody vychází z faktu, že mnohé charakteristiky člověka (fyziologické a behaviorální) jsou jedinečné a neměnné. Tato diplomová práce se zabývá přihlašováním do sítě pomocí biometrické metody otisku prstů.

V první kapitole je řešena problematika biometrie, její obecný popis, postupy získávání jednotlivých vzorků pro následnou verifikaci či identifikaci. Dále je zde uveden stručný přehled jednotlivých biometrických metod. Největší důraz je kladen na popis metody otisku prstů, je zde uveden nejen obecný popis biometrické metody, ale i popis jednotlivých snímačů.

V druhé kapitole jsou popsány jednotlivé síťové protokoly, které slouží k přihlašování do sítě. Je zde uveden přehled základních protokolů, jejich vlastnosti a využití.

Třetí kapitola je zaměřena na praktickou část, ve které je popsán návrh pracoviště pro získávání otisku prstů. Zde je uveden popis čtečky otisku prstů Eikon, instalace a nastavení potřebného softwaru pro snímání jednotlivých vzorků otisku prstů pro bezpečné přihlášení do sítě.

Poslední kapitola je pojata jako grafická prezentace řešené problematiky formou animace, ve které je ukázán postup instalace softwaru zvolené čtečky, nastavení softwaru, ukázka snímání jednotlivých vzorků a ukázka přihlášení do sítě.

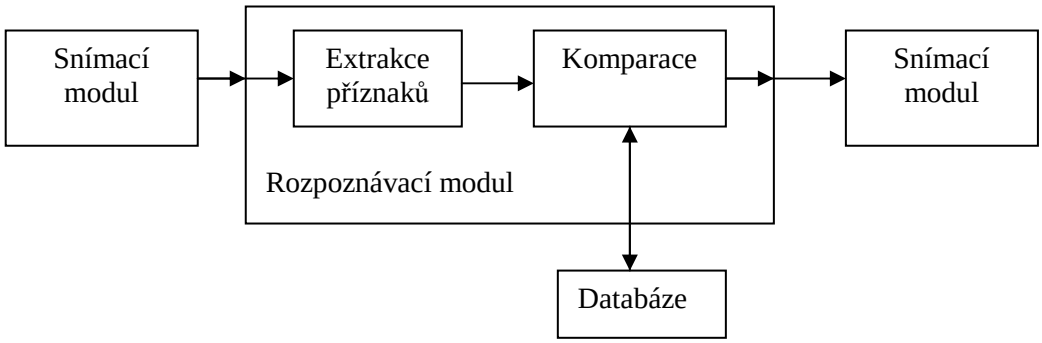
2 Biometrie

Biometrie je obor, který zkoumá člověka a jiné živé organismy podle jedinečných měřitelných charakteristik, a to buď anatomicko-fyziologických a nebo behaviorálních (tj. týkajících se chování). Biometrie se věnuje studiu metod vedoucích k rozpoznávání člověka na základě jeho unikátních proporcí nebo vlastností. Rozpoznávání lidí pomocí biologických charakteristik je metoda využívaná historicky, lidé se rozpoznávají pomocí vzhledu tváře nebo jsou známy otisky dlaní v jeskyních jako jakýsi podpis autora (některé z nich jsou až 30 000 let staré). S rozvojem počítačových technologií na konci 60. let se začalo i biometrické rozpoznávání člověka stávat automatizovaným. Biometrii lze výhodně využít pro rychlou a spolehlivou identifikaci osob a při ochraně budov, zboží a transakcí, ale jde také např. o vhodnou techniku pro zlepšení služeb poskytovaných zákazníkům v rámci věrnostních programů.

Typické oblasti využití biometrických metod a technologií jsou v současnosti následující: cestovní doklady, národní ID karty, automatické celní odbavení a pasová kontrola, fyzický přístup do budov, vozidel, ověřování totožnosti na dálku např. při nákupech po internetu či při využívání telefonního bankovnictví, používání bankomatu, přístup do sítě, do systému.

Příkladem biometrik jsou metody otisku prstů, geometrie tvaru ruky a obličeje, oční duhovka, či oční sítnice. Dále se využívá charakteristických vlastností chování, jsou to například dynamika stisku kláves nebo dynamika podpisu. V poslední době se také zaměřuje pozornost na zkoumání vlastnosti chůze, hlasu a detailně se rozebírá jejich možné využiti k identifikaci.

Technologie biometrik, tak jak je známe dnes, prošly obrovským pokrokem ve světě počítačů a stávají se nutnou součástí vzájemného propojení počítačů po celém světě. Díky použití biometrik se zvyšuje nejen míra zabezpečení, ale také komfort při jejich využívání. Při použiti hesla se předpokládá u uživatele jistá obezřetnost.



Obr.1 Princip činnosti biometrického systému

2.1 Základní pojmy

V biometrii se setkáváme s několika základními pojmy, zde je přehled těch nejpoužívanějších.

2.1.1 Verifikace

Systém verifikace řeší otázku : „Je to ten, za koho se pokládá?“. Uživatel zadá svou identitu a poskytne biometrická data, které se porovnají s daty uloženými v databázi. V závislosti na typu systému může být identita, kterou uživatel poskytuje ve formě uživatelského jména pro operační systémy (např. Windows, Linux), vlastní jméno nebo identifikační číslo (ID). Výstupem pak je verdikt systému, zdali je shoda, či nikoliv (match/ non match).

Verifikační systémy mohou obsahovat mnoho biometrických dat, ale vždy je otisk porovnáván pouze proti uloženému záznamu daného uživatele. Často se taková verifikace označuje 1:1 (jedna k jedné). Proces využívající uživatelského jména a biometrických dat je nazýván autentizací.

2.1.2 Identifikace

Systém identifikace řeší otázku: „Kdo je to?“ a nepožadují, aby uživatel určil svou identitu před biometrickým porovnáváním . Uživatel poskytne svůj otisk prstu, který se postupně porovnává z daného množství uložených dat v databázi, dokud nenajde shodu. Výstupem pak je identita uživatele – např. jeho jméno nebo ID. Identifikační systémy mohou obsahovat velký objem biometrických dat a identifikace je často označována jako 1:N, protože se jeden otisk porovnává proti množství uložených otisků.

Identifikační systémy se pak dále dělí na pozitivní a negativní. Pozitivní identifikační systémy jsou navrženy pro nalezení shody se zadanými biometrickými daty. Negativní identifikační systémy oproti tomu zajišťuji, že poskytnutá biometrická data v databázi nejsou. Takových systémů se využívá jako prevence uložení dvou stejných otisků prstů do jedné databáze. Takové systémy nalezneme nejčastěji v rozsáhlých aplikacích s použitím objemných databází. Výsledkem hledání v negativním identifikačním systému je tedy: „shoda nenalezena“. [4]

2.1.3 Srovnávání (Matching)

Srovnávání je komparace biometrických vzorů za účelem rozhodnutí jejich stupně shodnosti nebo úměrnosti. Proces srovnávání biometrických vzorů má za výsledek tzv. skóre (udává, jestli je vzorek shodný nebo ne), které je v mnoha systémech ohraničeno mezí, určující, zda je vzor shodný či nikoliv.

Skóre je hodnota, která nám určuje stupeň shody dvou porovnávaných vzorů. Skóre může mít spoustu variací a není přesně dáno žádným standardem. Shodnost vzorků nikdy nebude stoprocentní, proto je důležité, aby byly seřazeny všechny vzorky z databáze dle podobnosti se vzorem, se kterým je budeme srovnávat.

Mez je hodnota, která je předem dána administrátorem. Vzorek, který má skóre nižší je vyhodnocen jako vyhovující a zbytek za nevyhovující. Výsledek porovnání mezi skóre a mezí je rozhodnutí. Rozhodnutí mohou obsahovat vyhovující i nevyhovující vzory. Vše záleží na použitém systému.

2.1.4 Klasifikace chyb

Efektivnost biometrických rozpoznávacích systémů lze měřit mnoha statistickými koeficienty. Charakteristickými výkonnostními mírami jsou koeficient nesprávného přijetí, koeficient nesprávného odmítnutí, koeficient vyrovnané chyby, doba zápisu etalonu a doba ověření. Takových koeficientů existuje celá řada v závislosti na hloubce zkoumání problému.

FAR (False Acceptance Rate) – vyjadřuje poměr počtu shodných porovnání rozdílných vzorů ku celkovému počtu porovnání rozdílných vzorů. Otisky jsou rozdílné, ale jsou přijaty.

FRR (False Rejction Rate) – vyjadřuje poměr počtu porovnání vzorů osoby A vedoucí k neshodě ku celkovému počtu porovnání vzorů osoby A. Otisky jsou shodné, ale jsou zamítnuty.

Tyto dvě chyby dohromady charakterizují přesnost rozpoznávacího systému, který se využívá pro určeni jeho prahové úrovně. Platí nepřímá úměra těchto hodnot tzn. čím je menší hodnota FRR, tím je naopak větší hodnota FAR a naopak, proto hledáme hodnoty, kdy se FRR a FAR sobě co nejvíce blíží a samozřejmě jsou nejnižší.

Mezi další chyby patří:.

EER (Equal Error Rate) – odpovídá bodu úrovni, kde FRR = FAR.

FTA (Failure To Acquire rate) – definováno jako očekávaný poměr transakcí, pro které systém nemůže získat nebo nalézt obraz v dostačující kvalitě.

FIR (False Identification Rate) – udává pravděpodobnost, že při procesu identifikace je biometrická veličina (vlastnost) nesprávně přiřazena k některému referenčnímu vzorku. Přesná definice závisí na principu, kterým se přiřazuje pořízený vzorek k referenčnímu, jelikož se často stává, že po srovnávacím procesu vyhovuje více než jeden referenční vzorek, tzn. překračuje rozhodovací práh.

FTE (Failure To Enroll rate) – je to předpokládaný poměr populace, pro kterou systém není schopen opakovaně generovat vzory.

2.2 Biometrické technologie

V praxi se využívá mnoho metod k identifikaci osob. Ještě než se budu zabývat jednotlivými technologiemi, tak uvedu pár základních pojmů.

2.2.1 Základní pojmy

Biometrický vzorek – jde o odraz anatomicko-fyziologických nebo behaviorálních charakteristik člověka. Za biometrický vzorek považujeme např. otisk prstu, dlaně, kapku krve, podpis, slinu, křivku EKG apod.

Biometrické charakteristiky, data – jsou to všechny měřitelné údaje z biometrického vzorku. Daktyloskopický otisk prstu se skládá z množiny různě tvarovaných papilárních linií, které se rozvětvují, končí nebo kříží. Tyto všechny údaje je možno popisovat, měřit.

Biometrické markanty – je to část biometrických charakteristik, jež lze efektivně využít pro identifikaci nebo verifikaci. Například v otisku nalezneme charakteristické markanty, jako jsou začátek a konec linie, můstek, křížení, dvojitá nebo trojitá vidlice apod. V biometrickém vzorku je zpravidla vždy větší množství upotřebitelných markantů, než je pro identifikaci nebo verifikaci potřebné.

Biometrická šablona – je tvořena z naměřené hodnoty, charakteristiky, funkční závislosti apod., minimálního počtu markantů, které plně postačují pro jednoznačnou identifikaci nebo verifikaci. Biometrická šablona je konečným výsledkem maximální formalizace a optimalizace biometrického vzorku pro identifikační nebo verifikační účely. Biometrická šablona se ukládá na nosiče informací např. na magnetické proužky, čipy, do počítačových databází apod. Velikost šablony se udává v bytech. Na základě šablon probíhá automatizované vyhodnocování verifikace nebo identifikace.

Každé biometrické zpracování má pět základních etap:

– sběr biometrických dat
– přenos dat
– zpracování naměřeného signálu
– proces rozhodování
– uložení dat

Sběr dat

Biometrické zpracování začíná měřením anatomicko-fyziologických nebo behaviorálních charakteristik člověka, tzn. sběrem biometrických dat. Základním předpokladem identifikace nebo verifikace je jednoznačnost identifikačních charakteristik, jejich měřitelnost a časová stálost. Sběr dat probíhá pomocí snímacího senzoru, tím může být kamera, speciální čidlo, mikrofon, mechanický otisk prstu apod.

Přenos dat

Některé biometrické aplikace sbírají data na jednom místě a skladují nebo zpracovávají na jiném místě. Z tohoto důvodu je nutno zabezpečit přenos dat. Biometrické aplikace pracují s poměrně velkými objemy dat. Aby přenos dat a jejich uložení bylo rychlé a kladlo malé nároky na skladovací prostory, dochází ke komprimaci a poté k dekomprimaci dat. Proces komprimace a dekomprimace způsobuje určité ztráty, které se obecně zvětšují s rostoucím komprimačním poměrem. Pro různé biometrické technologie se používají různé kompresní techniky.

Zpracování signálu

Zpracování signálu se skládá z extrakce šablony, kontroly kvality a porovnávání v databázi s ostatními vzorky.

Extrakce šablony má za úkol získat všechny biometrické charakteristiky z dat nasnímaných pomocí senzorů. Také má za úkol rozlišit jednoznačné a dostatečné identifikační markanty a odfiltrovat rušivé vlivy, jako jsou např. šum, redundantní informace apod. Extrakce markantů probíhá z dekomprimovaného biometrického vzorku a je nezávislá na komprimačních a dekomprimačních algoritmech. Proces extrakce je zpravidla automatizován a jeho cílem je definování jednoznačných identifikačních charakteristik. Výsledkem extrakce je tzv. šablona, obsahující údaje, které tvoří specifičnost prověřovaného jedince pomocí zvolené biometrické metody a splňují základní identifikační podmínky unikátnosti, přesnosti, časové neměnnosti apod. Koncepce šablony je jedním ze základních pilířů biometrické aplikace. Extrakce markantních charakteristik má nevratný charakter, tzn. že není možné restaurovat původní obraz biometrického vzorku. V databázi jsou tedy uloženy jen dostačující identifikační informace. Tím je zaručena ochrana soukromí osob a osobních údajů. V níže uvedené tabulce je uveden přehled biometrických metod a extrakce charakteristických markantů.

Biometrická metoda	Extrakce charakteristických markantů.
Otisky prstů	Umístění a směr charakteristických bodů otisku (rozdvojení papilárních linií, jejich tvary apod.).
Hlas	Frekvence, inotace, trvání jednotlivých hlasových charakteristik.
Tvář	Relativní pozice a tvar nosu, očí, lícních kostí.
Ucho	Velikost, tvar ucha, vzdálenost anatomických bodů vnějšího boltce.
Oční duhovka	Rýhování a proužkování duhovky, geometrické obrazce.
Oční sítnice	Tvar markanty krevního řečiště v sítnici.
Geometrie dlaně a prstů	Délka a šířka kostí a kloubů dlaně a prstů.
Podpis	Rychlost, směr jednotlivých tahů, dynamika, vzhled podpisu.
Dynamika psaní na klávesnici	Pořadí kláves, časové intervaly mezi jednotlivými úhozy.

Tab. 1. Přehled biometrických metod a extrakce charakteristických markantů

V druhém kroku dochází ke kontrole kvality. Po extrakci identifikačních charakteristik, někdy dokonce před ní nebo během ní, potřebujeme vědět jestli je daný vzorek dostatečně kvalitní. Jestliže nasnímané charakteristiky jsou nějak nedostatečné, tak je potřeba opakovat nasnímání nových, kvalitnějších, charakteristik.

Ve třetím kroku dochází k porovnání šablon. Extrahované, kvalitní charakteristiky vzorku jsou odeslány do porovnávacího procesu. Porovnávání probíhá mezi šablonou právě nasnímaného vzorku a šablonami již dříve nasnímaných a do databáze uložených vzorků. První ukládání tzv. referenční šablony do databáze se v praxi nazývá zavádění šablony. Cílem porovnávání šablon je ztotožnit načtenou šablonu s jednou nebo více šablonami, uloženými v databázi. Uložené šablony mohou být již spojeny s identitou osoby např. osoby, jež mají oprávnění k přístupu do nějakého objektu, systému atd. Oprávněná osoba má v databázi uloženou svou vlastní referenční šablonu, která je zaváděna jako první. Porovnání s touto šablonou pak rozhoduje, jestli daná osoba bude uznána jako oprávněná osoba či neoprávněna. Příkladem porovnávání může být nalezení pachatele trestného činu, kdy jsou v databázi uloženy referenční šablony zločinců. Porovnáním se pak ztotožňují stopy neznámého pachatele s evidovanými charakteristikami známých osob a tím se identifikuje pachatel, pokud dojde ke shodě. [1]

Rozhodování

V rozhodovacím procesu se stanovuje shodnost šablony se šablonou referenční. Míra shody se stanoví na základě měřitelných charakteristik, vypracovaných metod a algoritmů. Při rozhodování se stanovuje identifikační závěr, ve kterém je patrno, zda lze nebo nelze osobu autorizovat.

Uložení dat

Jde o poslední etapu zpracování dat. Podle typu použitého biometrického systému se ukládá jedna nebo více referenčních šablon. Jelikož biometrické systémy pracují obecně s velkými objemy dat, tak ukládání dat má dvě koncepce. První uchovává originální otisky prstů a druhá koncepce pracuje s datově menšími šablonami, které jsou ze vzorků odvozeny pomocí algoritmů.

2.3 Otisky prstů

Identifikace na základě otisku prstů je jednou z nejznámějších a nejvíce publikovaných biometrických metod. Otisk prstů se používá pro jeho jedinečnost a stálost v čase. Identifikace otisku prstů je s oblibou používaná především pro relativní jednoduchost získání srovnávacího vzorku, pro vysoké procento použitelné populace, dále pro četnost zdrojů ze kterých lze získat vzorek (10 prstů) a také protože jde již o zavedenou metodu s velkou databází.

Používání otisku prstů (přesněji obrazců papilárních linií na vnější straně prstů rukou, nohou a dlaní) jako metody pro identifikaci se začala používat už na konci 19. století, kdy Sir Francis Galton nalezl a definoval některé charakteristické body na prstu, které mohou sloužit k identifikaci člověka. Tyto „Galtonovi body“ položily základ vědnímu zkoumání otisku prstů, který byl rozvíjen po celé století. [1]

Metody zachycení otisku prstů

– otisk získaný pomocí inkoustu a papíru
– statické snímání
– snímání šablonováním

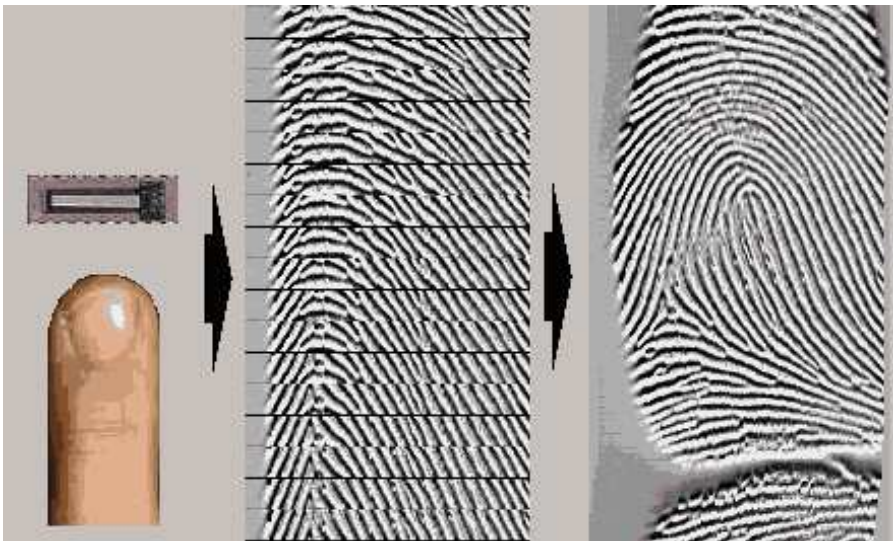
Otisk získaný pomocí inkoustu a papíru je klasická metoda (rolled finger). Tato metoda se používá ve forenzní sféře, policií při vyšetřování, apod. Používá se inkoustu a papíru. Prst se po papíře roluje, aby se získal otisk celého prstu (prakticky od nehtu po nehet) s co možná nejvíce použitelnými markantami, aby se tím zvýšila i rychlost rozpoznání otisku.

Statické snímání

Jedná se o nejběžněji používanou metodu snímání otisku prstů. Uživatel přitiskne svůj prst na senzor bez jakéhokoliv pohybování s ním. Výhodou této metody je nesporně jednoduché ovládání (stačí pouze přiložit prst). Na druhou stranu je zde řada nevýhod: přílišným tlakem prstu může uživatel rozlomit snímací čočku (obzvlášť je-li doba snímání delší, uživatel znervózní a přitlačí více), přiložení prstu a jeho současné pootočení vede k deformaci pokožky a celého otisku, senzor se lehce zašpiní (nehygieničnost) a na senzoru můžou zůstat latentní otisky.

Snímání šablonováním

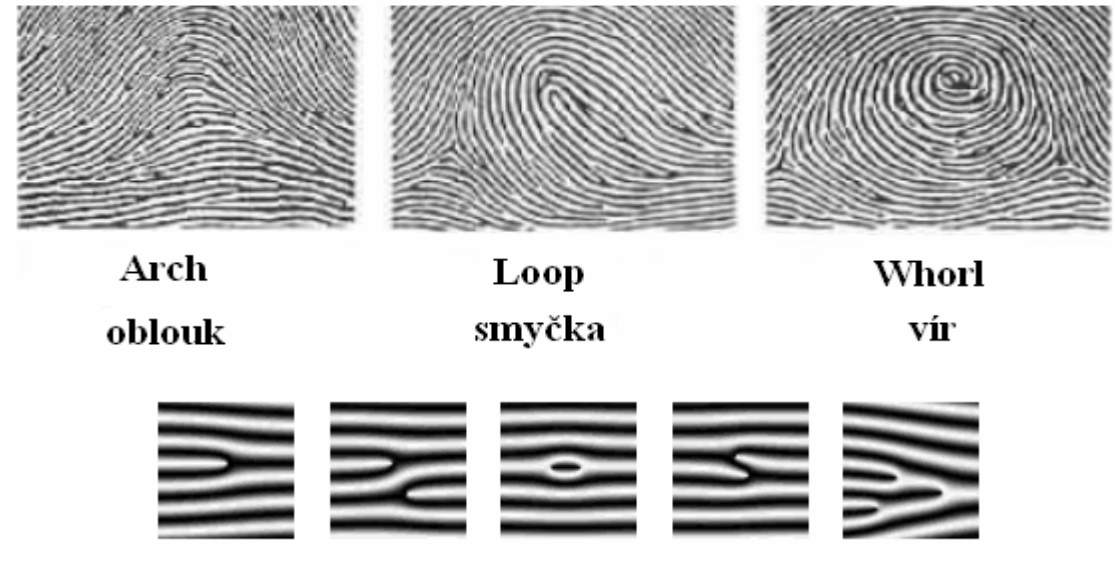
Uživatel přejíždí prstem po senzoru, který snímá a opětovně skládá obraz pomocí pásů (Obr.2.). Používá-li se křemíkový snímač, pohybuje se i cena v oblasti křemíkových součástek. Redukovat cenu lze právě využitím šablonovaného snímání tím, že snímač bude mít tvar úzkého pruhu. Celková cena pro pořízení otisku prstů se poté výrazně nižší. Výhody šablonovaného snímání jsou: snímač zůstává stále čistý, jelikož každý sejmutý pruh vyčistí senzor, na snímači nezůstávají skryté (latentní) staré otisky, uživatel nemá pocit ‚zanechaného' otisku prstů a snímání je rychlé. Nevýhodou je, že obsluha takového zařízení není intuitivní a uživatel se musí naučit určitý postup.



Obr.2. Ukázka snímání otisku prstu šablonováním

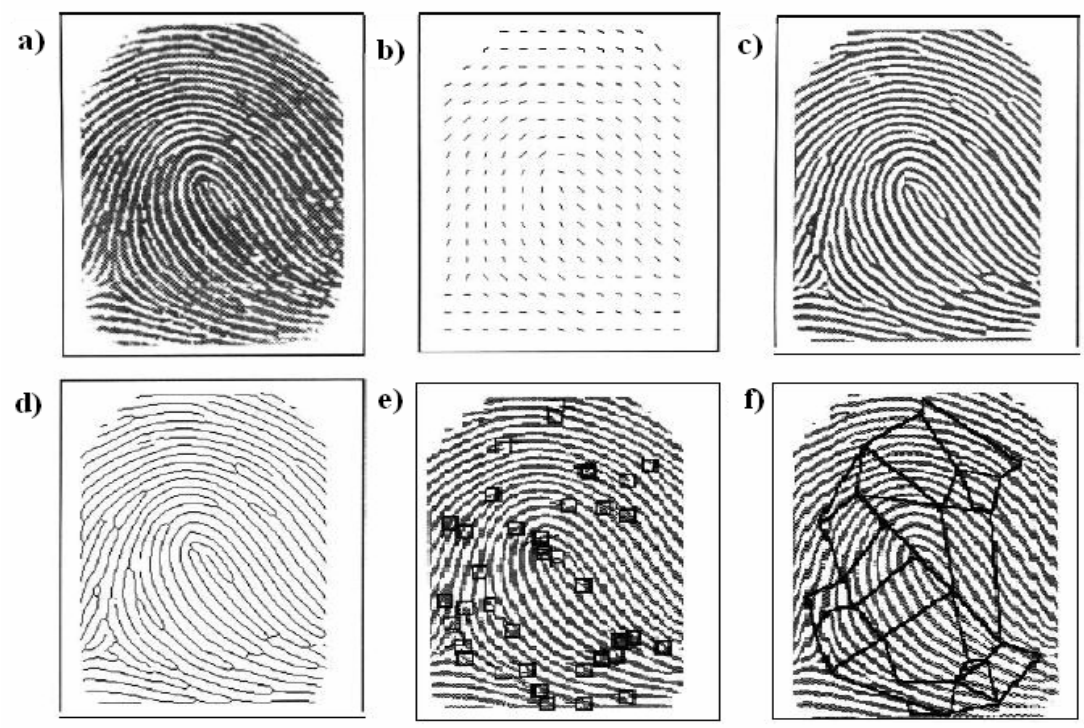
Používané algoritmy u snímačů otisku prstů – srovnávací metody

Většina algoritmů využívá existence markant, specifických bodů jako je zakončení linie, rozvětvení linie, bod (ostrov), jezero, výběžek (osten) nebo zkřížení, což jsou detaily třech hlavních vzorů (seskupení papilárních linií). Jedná se o smyčky, víry a oblouky (loop, whorl, arch) viz Obr.3.



Obr.3. Seskupení papilárních linií

Často používaný algoritmus vytváření tzv. markantografu pracuje na vytvoření obrazce spojnicemi mezi nalezenými markantami. Postup je následující: obraz originálu otisku prstu je podroben filtru orientace markant, následné počítačové binarizaci dat, zeslabení linií, nalezení markant a vytvoření markantografu (viz Obr.4.)



Obr.4. a) originální otisk b) filtr orientace markant c) binarizace d) zeslabení e) nalezení markant f) markantograf

Technologie snímačů otisku prstů

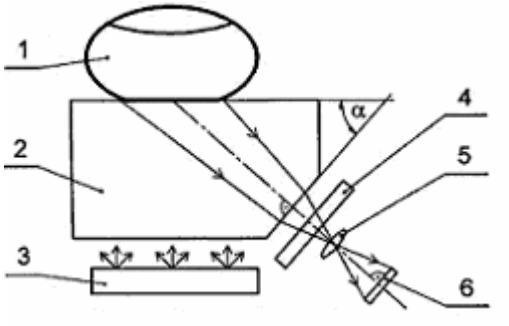
2.3.1 Optoelektronické snímače otisku prstů

Optoelektronické snímače díky svým vlastnostem a výhodám jsou vhodné především pro algoritmy rozpoznání založené na markantech (speciální útvary na otisku prstu, které tvoří papilární linie).

Princip činnosti je založen na rozdílném odrazu světla. Optický snímač zachycuje digitální zobrazení otisku pomocí viditelného světla (na rozhraní plochy hranolu a přiloženého prstu). Obraz otisku se přenese na maticový CCD detektor, následně je digitalizován a dále předán pro zpracování obrazu otisku. Pod vrstvou kde se přikládá prst (dotekový povrch) je vrstva fosforu, která osvětluje celou plochu prstu. Odražené světlo od povrchu prstu prochází luminoforní vrstvou k CCD maticovému detektoru,kde tam se vytvoří obraz otisku (z papilárních linií se světlo odráží, z rýhy nikoliv).

Nevýhodou je, že při znečištění nebo poškození prstu může způsobit špatné vykreslení prstu. Dále první otisk, který se vytvoří, může při dalším snímání zachytit tento první otisk. Větší rozměry čtečky limitují implementaci do malých a přenosných zařízení.

Výhodou je vysoká kvalita, odolnost proti statickým výbojům a minimální vliv okolního prostředí.



1-přiložený prst
2-snímací hranol
3-osvětlovací soustava
4-optický filtr
5-snímací objektiv
6-maticový CCD detektor

Obr.5. Optoelektronický snímač

2.3.2 Kapacitní snímače otisku prstů

Princip činnosti využívá rozdílu kapacity mezi deskou snímače a povrchem prstu (vyvýšeniny a prohlubně). Snímač představuje jednu desku kapacitoru a druhou desku na jednotlivá místa na prstu. Otisk se tak z pixelů získá v digitální formě. Pro načtení obrazu přiložíme prst na citlivou plochu osazenou velkým množstvím elektrod. Ty převedou kapacitně otisk prstu na digitální obraz, který se dál zpracovává. Papilární linie jsou k podložce více přilehlé než mezery mezi nimi, takže mají vyšší kapacitní odpor.

Nevýhodou je:

– malá doba životnosti (zničení snímače vlivem statické elektřiny) při práci ve vlhkém prostředí

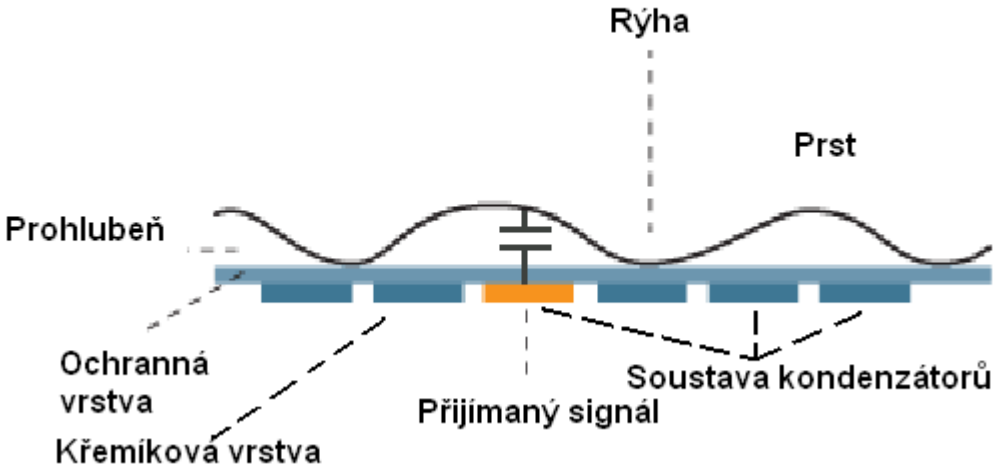
– snímače je většinou nutné měnit v rozmezí 3 let (není zase takový problém z hlediska ceny, ale spíše z organizačního hlediska)

Výhodou je:

– malý rozměr

– levná výroba

– jednoduchý princip funkčnosti



Obr.6. Kapacitní snímač

2.3.3 Teplotní snímače otisku prstů

Teplotní snímače obsahují malý citlivý čip (pyrodetektor). Pyrodetektor snímá rozdíl teplot mezi jednotlivými papilárními liniemi a prostory mezi nimi (výstupky). Proto, abychom získali obraz otisku prstu, musíme přejíždět prstem přes citlivou plochu. Na výstupu dostaneme obraz otisku ve formě digitálních pásů (frames). Digitální pásy se následně skládají do výsledného obrazu otisku.

Nevýhodou je :

– nízká kvalita, problémy s algoritmy pro zpracování markant

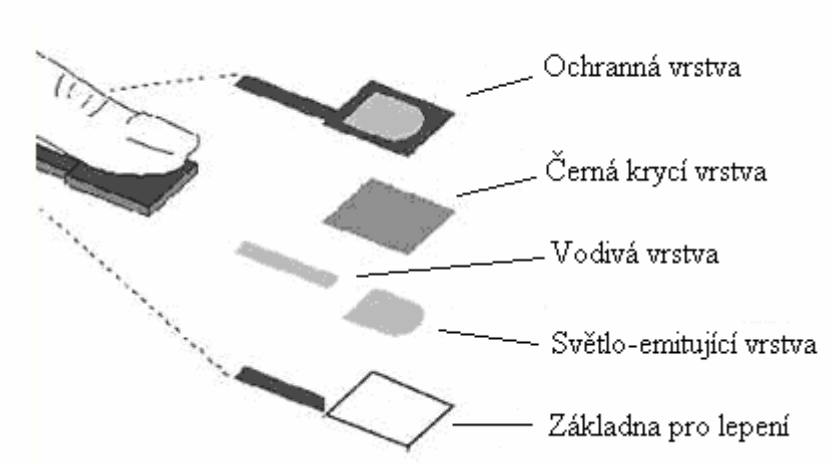
– snímání otisků pouze pohybem prstu, tím pádem po několika sejmutí může být pokaždé sejmuta jiná část prstu. Tím pádem je obtížné vytvořit databázi otisků.

– špatná kvalita obrazu otisku, teda není vhodná pro použití v přístupových systémech.

2.3.4 Elektroluminiscenční snímače otisků prstu

Elektroluminiscenční snímače jsou nejnovější technologií, která se objevila na trhu. Snímací plocha je tvořena několika vrstvami, přičemž z hlediska funkčnosti je nejdůležitější světlo eliminující vrstva, která eliminuje světlo v místech, kde na ni tlačí papilární linie prstu.

Výhodou elektroluminiscenčních snímačů jsou miniaturní rozměry, dobré rozlišení, které se pohybuje kolem 500 dpi a přijatelná cena. Podstatnou výhodou je také skutečnost, že kvalita otisku se nesnižuje, když je prst extrémně suchý. Nevýhody jsou většinou dány samotným konstrukčním řešením. Zatím se jedná o nižší odolnost vůči mechanickému poškození a náchylnost ke znečištění prachem či vodou.



Obr.7. Elektroluminiscenční snímač

2.3.5 Radiofrekvenční snímače

Princip činnosti spočívá v připojení generátoru střídavého signálu na 2 rovnoběžné desky (ty představují plochu snímače a ta druhá plocha otisku prstu). Jelikož je vlnová délka mnohem větší než délka desek, vyskytuje se pouze složka elektrického pole, bez pole magnetického. Pokud tedy jedna z desek bude náš otisk prstu, tvar pole se změní a bude kopírovat tvar linií tzn. výběžky a prohlubně. Vodivé prostředí mezi prstem a plochou je docíleno pomocí vodivé plochy kolem každého snímače, tzn. že i suché prsty nejsou problémem, jelikož se pracuje s živou tkání těsně pod povrchem pokožky. Zvlněním pole, které je způsobené přiloženým otiskem prstu, dopadá na senzory signál s rozdílnou velikostí signálu. Výběžky mají větší signál a tzv. údolí nižší signál.

Kapacitní senzory tak měří rozdílnou permitivitu mezi výběžky a údolími. Výhodou je odolnost vůči nečistotám, tzn. pokud jsou nečistoty v údolích, tak nepředstavují problém. Technologie trueprint je přizpůsobivá stavu kůže, pořizuje několik snímků, které jsou postupně optimalizovány až do doby přesného přijetí nebo odmítnutí snímků.

Požadavky na senzory

1) Vyhovující celkové rozměry – tento požadavek je snadno splnitelný u systémů určených pro přístup do místnosti, budov atd. Pro přístup do počítačů, notebooků apod. je již potřeba miniaturizace zásadní.

2) Dostatečně velká snímací plocha –je nutná pro záznam dostatečného počtu identifikačních znaků (markant), nebo plochy obrazu. Existuje malá skupina lidí, která má extrémně málo markant nebo má část markant vyhlazených prací.

3) Dostatečné rozlišení – požadavek na rozlišení je dán především použitým algoritmem na rozpoznání, požadavky na spolehlivost a nastavením chyb prvního a druhého druhu pro systém. Kvalitní obraz by neměl být zkreslený, měl by mít dostatečný kontrast a obsahovat pokud možno co nejširší škálu rozsahu šedé barvy.

4) Opakovatelnost dosažené kvality obrazu otisku prstů – pro dosažení dobrých výsledků při autentizaci z hlediska hodnot chyby prvního a druhého druhu je důležitá opakovatelnost kvality obrazu otisku. Posun obrazu otisku vzhledem k etalonu a jeho natočení musí být při pokusu o autentizaci minimální.

5) Dostatečná ochrana vůči napodobeninám – snímač sám o sobě nezabezpečuje dostatečnou ochranu vůči napodobeninám. Jedná se o slabé místo celého systému. Některé testy s napodobeninami vykazují dokonce lepší poměr FAR a FRR než původní lidské biometrie. Řešením je dodatečná ochrana pomocí kamer nebo fyzické přítomnosti ostrahy.

6) Uživatelská přívětivost – je základním požadavkem ve směru k uživateli systému a ergonomii snímače.

7) Odolnost vůči mechanickému poškození – většina snímačů je konstruována pro připojení k počítači, notebooku, atd., a neprošla zkouškami na odolnost vůči mechanickému poškození, ani zkouškami ve ztížených klimatických podmínkách, což je chyba.

8) Spolehlivost snímačů otisků prstu – je zjišťována především testy na chybu prvního a druhého druhu. Řada výrobců udává ovšem hodnoty, které nejsou dosažitelné ani teoreticky.

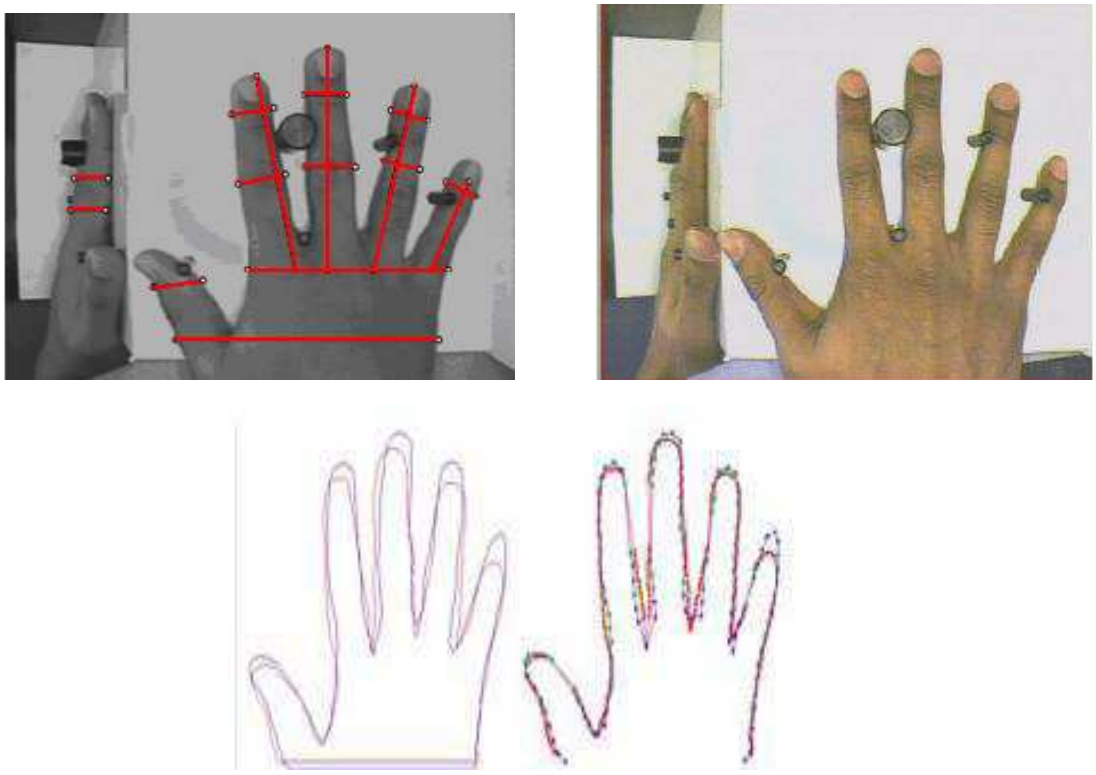
9) Životnost snímačů – jedná se o konstrukční prvky snímačů, u nichž je z principu omezena životnost. Jsou to především materiály, které chrání snímací plochu vůči poškození.

10) Cena snímače – je velmi variabilní v závislosti na řadě faktorů. Přesto je z výše uváděného rozboru zřejmé, že zřejmě nejdražší budou kvalitní optoelektronické snímače. Při realizaci konkrétního návrhu zabezpečení pomocí ACS je nutno zvážit všechny aspekty a vytvořit vhodný kompromis s požadavky zadavatele projektu. [8]

2.4 Geometrie ruky

Systém rozpoznávající geometrii ruky je nestarším implementovaným biometrickým principem. Vyvinul jej a nechal si je patentovat David Sidlauskas v roce 1985 a hned v příštím roce byli již systémy rozpoznávající geometrii ruky komerčně dostupné. V roce 1996 byly tyto systémy použity pro identifikaci na Olympijských hrách v Atlantě, kde zajišťovaly bezpečnost vstupu do olympijské vesnice. Jelikož ale není geometrie ruky příliš unikátní biometrickou vlastností, je její aplikace v bezpečnostní sféře omezena právě stupněm bezpečnosti, kterého chceme dosáhnout.

Zařízení pro rozeznávání geometrie ruky využívají jednoduchého principu měření a tří dimensionálního snímání délky, šířky, tloušťky a povrchu ruky konkrétního člověka umístěné na podložce s pěti polohovými kolíky (viz Obr.8.) pomocí CCD kamery.[1]



Obr.8. Snímání ruky pomocí CCD kamery

Obr.9. Ruka se zrcadly snímaná CCD kamerou

Na obrazu ruky lze najít přes 31 000 polohových bodů a provést 90 různých měření vzdáleností. Vybrané měřené informace se ukládají do 9 bitového souboru, což činí tyto systémy velice výhodné z hlediska nízkého požadavku na paměť systému. Biometrické systémy založené na verifikaci geometrie ruky jsou používány v různorodých aplikacích docházkových systémů a přístupových systémech, kde jsou poměrně velmi rozšířené. V USA je systém normalizován ANSI INCITS 396–2005.. FRR: <0.1%; FAR: 0.1%, Čas verifikace: 1 až 2 sekundy; Míra spolehlivosti: střední

Výhodou této technologie je, že je to uživatelsky a technologicky velmi jednoduchá a rychlá metoda, lehce použitelná i pro nevidomé.

Nevýhodou je, že skener nelze miniaturizovat, má velkou náchylnost na povětrnostní podmínky a tuto technologii lze využít pouze pro verifikaci.

2.5 Geometrie tváře

Verifikace obličeje je dnes nejvíce zkoumanou metodou, neboť problematika identifikace osob dle tváří je velmi obsáhlá. Rozpoznávání je založeno na srovnávání obrazu sejmutého kamerou s obrazem, který je uložen v centrální databázi. K jednoznačné identifikaci slouží většinou tvar obličeje a poloha opticky významných míst na tváři, jako jsou oči, nos, ústa či obočí. Obraz v počítači může být někdy uložen jako matice jasových úrovní, častěji je však diskriminován nějakou funkcí, která snižuje redundanci dat. Neuchovává se tedy přesná poloha očí, nosu a rtů, ale ukládá se jen vzdálenost očí, vzdálenost rtů od nosu, úhel mezi špičkou nosu a jedním okem, atd.

V současné době je známo několik technik rozpoznávání tváří. K těm významnějším a nejvíce používaným patří metoda měření geometrických vlastností a metoda porovnávání

šablon. Všeobecně se věří, že po zdokonalení systému rozpoznávání obličeje by mohli odpadnout mnohé, méně efektivní systémy (např. docházkový systém do zaměstnání). Je však pravdou, že během výzkumů se velmi často špatně specifikovaly požadavky, což vedlo k nízké funkčnosti a efektivnosti systému. Jsou však známy i případy, kdy byly požadavky na systém tak přemrštěné, že bylo obtížné, respektive naprosto nemožné takový systém realizovat. Proto je nutné si uvědomit, jak vysoké nároky je nutné klást na daný identifikační systém. Je obrovský rozdíl v realizaci systému, který porovnává dva statické obrazy a systému, který ověřuje totožnosti jednotlivce nacházejícího se ve skupině lidí. Atraktivnost rozpoznávání obličejů je z hlediska praktického užívání pochopitelná, ovšem je nezbytné být realistický ohledně vyhlídek této technologie. Doposud neměli obličejové rozpoznávací systémy v praktických aplikacích velký úspěch. [1]

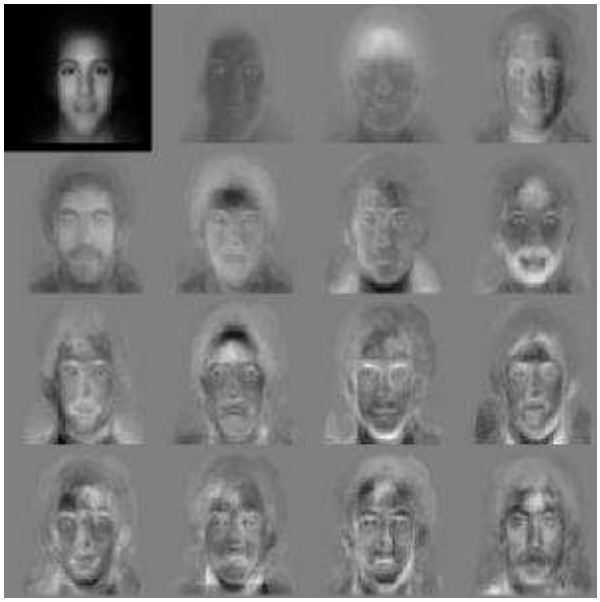
Existují dva odlišné přístupy rozpoznávání geometrie tváře: geometrický (založený na rysech tváře) a fotometrický (založený na vzhledu obrazu tváře). Tři nejlépe prozkoumané a studované algoritmy rozpoznávání tváře jsou:

– analýza hlavních částí (PCA - Principal Components Analysis)

– lineární diskriminační analýza (LDA - Linear Discriminant Analysis)

– elastický srovnávací diagram (EBGM - Elastic bunch graph matching)

PCA využívá vektorů tváře odvozených s kovarianční matice pravděpodobnostní distribuční funkce k vytvoření šablony vhodné pro srovnávání. Každá tvář lze rozdělit na tzv. eigenfaces (vzory tváří - matice jasových úrovní) a poté jde opět složit (viz. Obr.9.). Každá eigenface je reprezentována pouze číslem, tudíž se namísto obrázku ukládá pouze číslo.

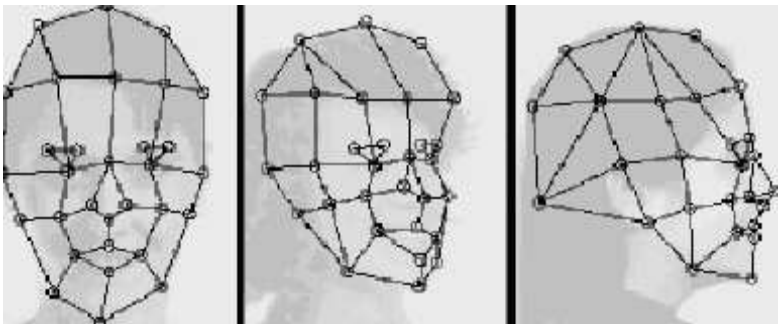


Obr.9. Standardní eigenfaces používané pro rozložení obrazu

LDA je metoda, kdy se třídí pořízené obrazy tváří do skupin. Cílem je maximalizovat rozdíly mezi jednotlivými skupinami a minimalizovat rozdíly v každé skupině. Každý blok snímků reprezentuje jednu třídu (viz Obr.10.).

Obr.10. Příklad šesti tříd užitím LDA

EBGM byla vyvinuta důvodu, že předešlé metody nemohou uvažovat nelineární charakteristiky jako je osvětlení okolí, pozice hlavy anebo výraz tváře (úsměv, zamračení). Na obličeji se definují uzlové body, které se poté propojí a tím definují linie tváře v prostoru, vznikne tím souřadnicová síť obličeje (viz. Obr.11.). Samotné rozpoznávání pak probíhá tak, že systém pomocí filtru uzlových bodů reaguje na jednotlivé snímané tváře a může je pak porovnávat a vyhodnocovat. Problémem je přesnost lokalizace orientačních bodů na tváři, řešením může být kombinace s PCA nebo LDA metodou. FRR: <1%; FAR: 0,1%, Čas verifikace: 3 sekundy, Míra spolehlivost: střední.[1]



Obr.11. Síť vytvořená elastickým mapováním

Identifikace osob dle geometrie tváře je dnes velice moderním a expandujícím principem. Dochází k její integraci na letištích, nádražích, rušných ulicích, náměstích a všeobecně na místech, kde by se mohli pohybovat pohřešované a hledané osoby apod.

Nepřesnosti detekce tváře

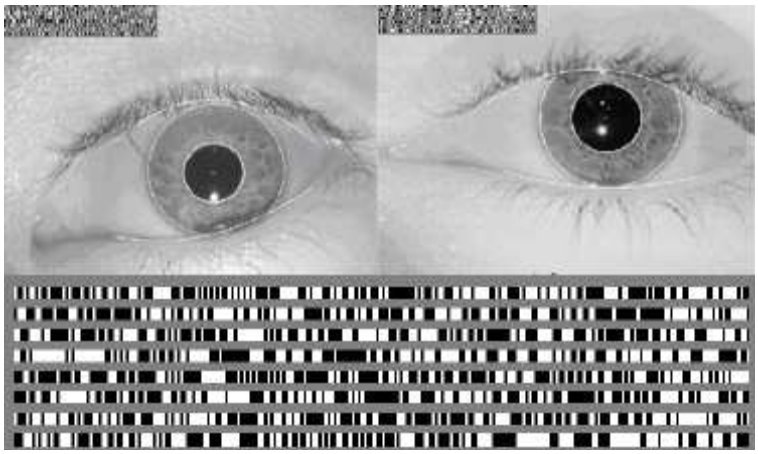
Systémy, které jsou schopny poznávat tváře, omezují rozsah možného správného výběru na třetinu všech možných kandidátů pozitivní identifikace. Jestliže je tvář osoby vyfotografována venku, a to z úhlu 45 stupňů, typický automatizovaný systém selhává v 80 procentech případů. Vliv na nepřesnosti má také proměnlivost osvětlení, způsobovaná odlišností oblečení, vede k tomu, že ve 40 procent případů nedokáže systém danou osobu identifikovat na základě uložené fotografie. Tato technologie může být nápomocná při prohledávání databází fotografií osob, ale fotografie musejí obsahovat záběr celé tváře a musí být k dispozici dostatečné množství manuálních pracovníků, kteří budou schopni spojit fotografii hledaného jedince s fotografií v databázi.

2.6 Duhovka oka

První patent je datován k roku 1994 a vyvinul ho americký Úřad pro jadernou bezpečnost včele s Dr. Johnem Daugman. Oční duhovka každého člověka je co do podobnosti unikátní. Jde o pigmentovanou membránu obklopující zřítelnici oka. Duhovka kontroluje úroveň světla, které vstupuje do oka. Černý otvor ve středu duhovky se nazývá pupila (panenka). Duhovka je spojena s jemnými svaly, které duhovku bud rozšiřují nebo zužují. Je plochá a rozděluje oko na přední a zadní část. Barva duhovky je způsobena barvivem, které se nazývá melanin.

Obr.12. Duhovka a její popis

Snímání duhovky vyžaduje velice kvalitní digitální kameru a infračervené osvětlení oka. Během snímání se duhovka mapuje do fázorových diagramů, které obsahují informace o orientaci, četnosti a pozici specifických plošek. Tyto informace pak slouží k vytvoření duhovkové mapy (viz Obr.13.) a šablony pro identifikaci.



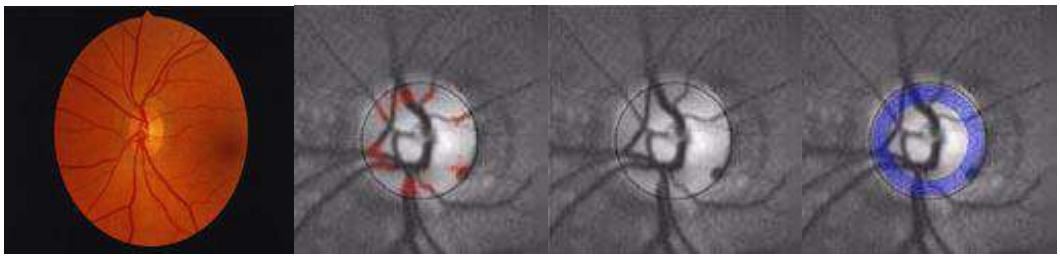
Obr.13. Lokalizování duhovky a její piktografické znázornění

Při verifikačním procesu se porovnává žadatelova mapa duhovky s referenční pomocí testu statistické nezávislosti. Pokud je pouze méně než jedna třetina dat odlišná, test statistické nezávislosti selhal, což znamená, že vzorky jsou ze stejné duhovky. FRR: 0,00066%; FAR: 0,00078%, Čas verifikace: 2 sekundy, Míra spolehlivosti: vysoká.[1]

2.7 Sítnice oka

Jedná se o světlocitlivý povrch zadní strany oka. Je složen z nervových buněk tyčinek a čípků, které převádějí přicházející světelné paprsky na nervové signály. Tyčinky poskytují černobílé a čípky barevné vidění. Oční nerv, společně s artérií sítnice, vystupují z oka v místě, kde se nenacházejí žádné tyčinky ani cípky. Označujeme jej pojmem slepá skvrna. Popisovaná biometrická technologie porovnává právě strukturu sítnice v okolí slepé skvrny. Snímání se provádí zaměřením infračerveného paprsku o nízké intenzitě skrz zornici na vzor cév nacházejících se na zadní straně oka. Sítnice je u této vlnové délky průhledná, zatímco cévy sítnice infračervené světlo reflektují.

Používání této metody vyžaduje od uživatele, aby se díval do přesně vymezeného prostoru, což může být pro některé osoby nepříjemné a někdy až nemožné, pokud používají brýle. Z těchto důvodů nemá tato metoda rozšířenou oblast používání a její použití se shrnuje na oblasti vůbec nejvyššího stupně zabezpečení. FRR: 0,4%; FAR: 0,001%, čas verifikace: 1,5 až 4 sekundy, Míra spolehlivosti: vysoká.



Obr.14.Lokalizování sítnice a znázornění charakteristických parametrů

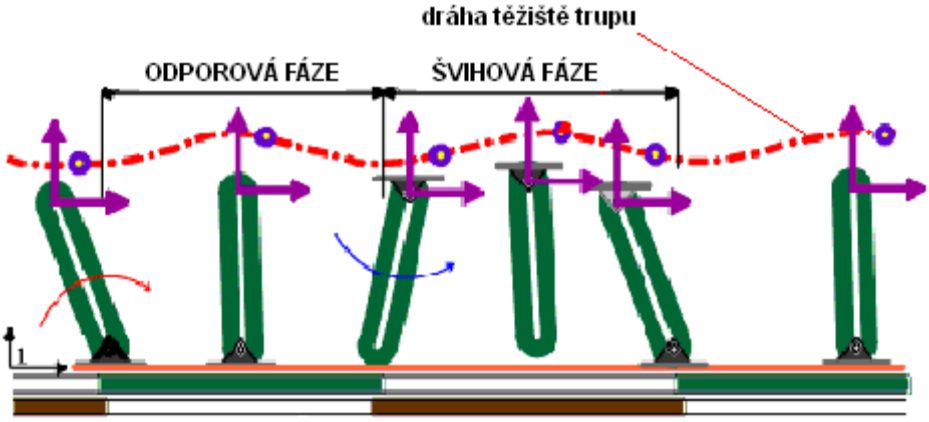
Obr.15. Snímač sítnice oka

2.8 Dynamika chůze

Stejně jako otisk prstu nebo duhovka oka je i pohyb člověka jedinečný a svým způsobem neměnný v relativně širokém časovém období. České kriminalistice a jejímu výzkumu patří přední místo ve světě ve vývoji identifikace člověka podle stylu chůze, tedy „pohybu po dvou nohách“. Velký podíl na rozvoji této metody má i rozmach záznamové a snímací techniky. Stejně jako při identifikaci podle ručního písma je rozlišovacím znakem jedinců různý dynamický stereotyp. U písma se jedná o stereotyp ruky a chůze celého pohybu těla.

Tato metoda má obrovský význam při identifikování pachatelů loupežných přepadení, jimž je zcela zbytečné jakékoliv maskování nebo převleky. Další význam tato metoda nabývá při současném prudkém rozvoji nasazování průmyslových kamer na nejrůznější rušná místa (letiště, náměstí, nádraží, multifunkční komplexy atd.). Její uplatnění je tedy pouze ve forenzní sféře, kde však dosud stále neexistuje databáze srovnávacích materiálů. Celá metoda pracuje na základě porovnávání křivek drah, které opisují určité body na lidském těle, hlavně jeho těžiště. Jelikož je každý člověk jedinečný svým pohybovým svalově kosterním systémem a svým

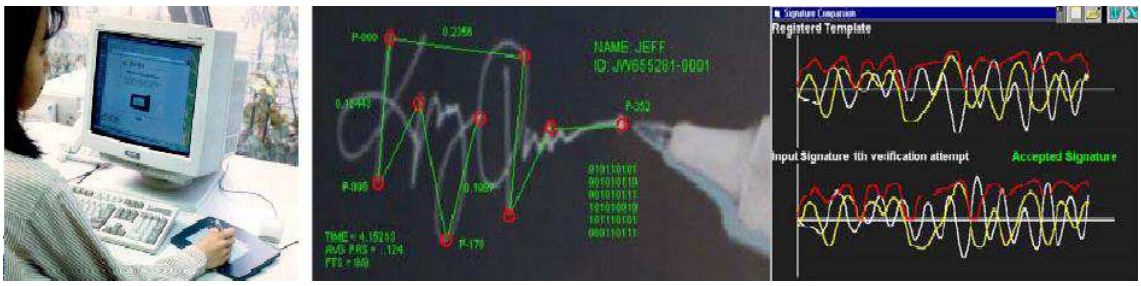
dynamickým stereotypem, jsou i křivky uvažovaných bodů unikátní a vhodné pro srovnávání a 1:1 identifikaci. Způsob vytváření těchto křivek je na Obr.16. [1]



Obr.16. Postup vytváření dráhy těžiště trupu

2.9 Dynamika podpisu

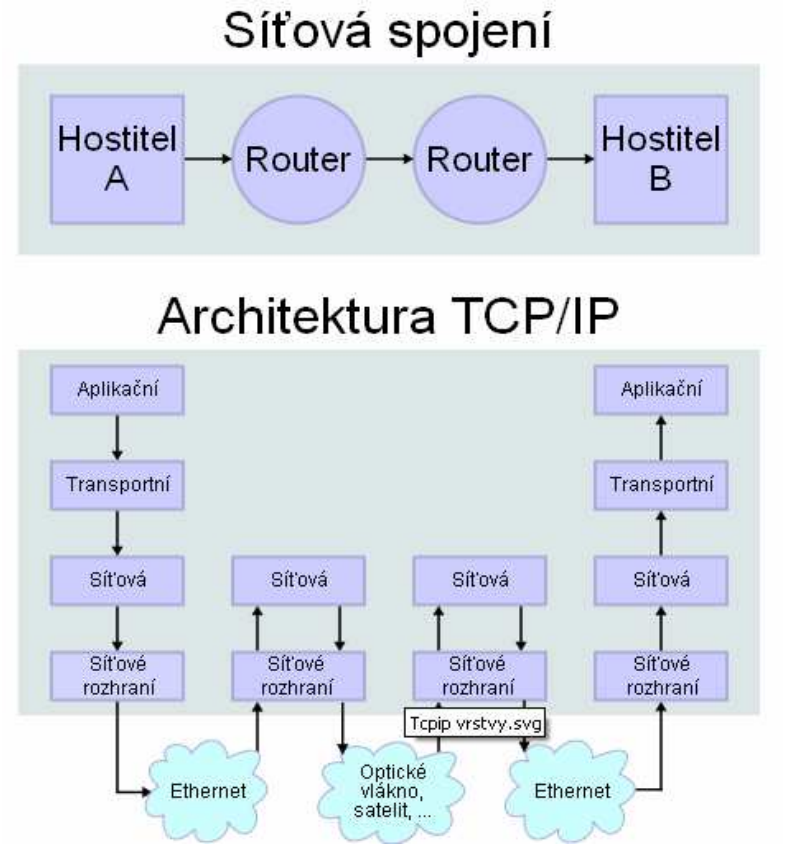
Tato metoda je datována k roku 1977 a využívá jedinečnosti kombinace anatomických a behaviorálních vlastností člověka. Základními dynamickými vlastnostmi jsou rychlost, akcelerace, časování, tlak a směr tahu, které jsou zaznamenávány v trojrozměrném souřadnicovém systému (viz Obr.17). Osy ‚x' a ‚y' slouží k určení rychlosti a směru tahu, souřadnice ‚z' určuje tlak na podložku. Na rozdíl od statického obrazu podpisu, který může být naučen a napodobován, je nemožné se dynamiku podpisu pouze z obrázku naučit. Výhodou je i snadné integrování zařízení do již existujících systémů (stačí PDA a vhodný SW). Naopak nevýhodou je, že tyto systémy jsou schopné zvládat pouze verifikační principy.



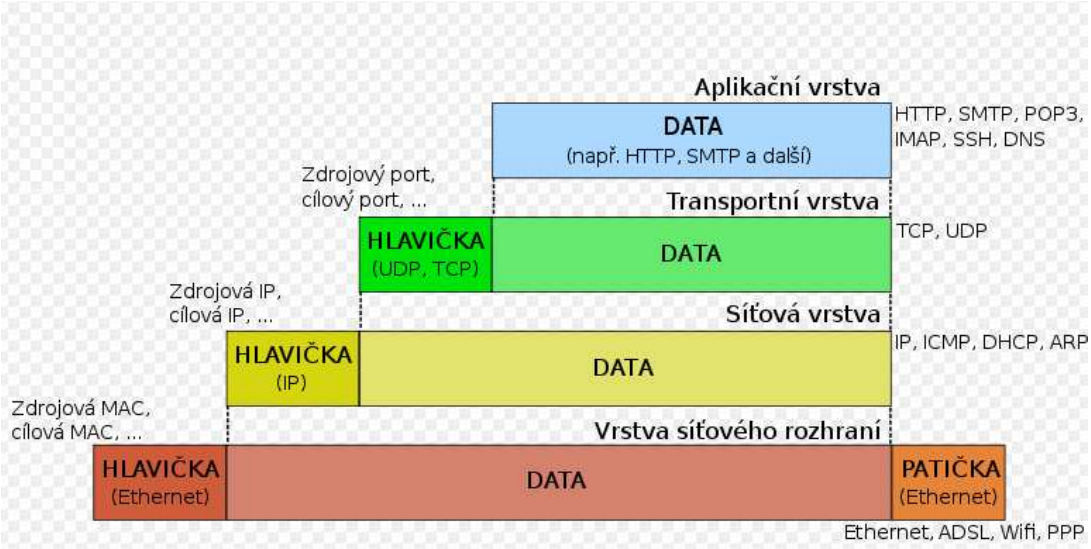
Obr.17. Ukázka dynamiky podpisu

3 Způsoby přihlašování do sítě

Protokoly TCP/IP slouží pro komunikaci v počítačové síti a jsou hlavním protokolem celosvětové sítě Internet.



Obr.18. Architektura TCP/IP přenos mezi dvěma hostiteli prostřednictvím dvou routerů.



Obr.19. Schéma zapouzdření aplikačních dat na vrstvách TCP/IP

Vzhledem ke složitosti problémů je síťová komunikace rozdělena do tzv. vrstev, které znázorňují hierarchii činností. Výměna informací mezi vrstvami je přesně definována. Každá vrstva využívá služeb vrstvy nižší a poskytuje své služby vrstvě vyšší. Komunikace mezi stejnými vrstvami dvou různých systémů je řízena komunikačním protokolem, za použití spojení vytvořeného sousední nižší vrstvou. Architektura umožňuje výměnu protokolů jedné vrstvy bez dopadu na ostatní. Příkladem může být možnost komunikace po různých fyzických médiích - ethernet, token ring, sériová linka.[2]

Architektura TCP/IP je členěna do čtyř vrstev (na rozdíl od referenčního modelu OSI se sedmi vrstvami):

– vrstva síťového rozhraní (network interface)

– síťová vrstva (network layer)

– transportní vrstva (transport layer)

– aplikační vrstva (application layer)

Vrstva síťového rozhraní

Nejnižší vrstva umožňuje přístup k fyzickému přenosovému médiu. Je specifická pro každou síť v závislosti na její implementaci. Příklady sítí: Ethernet, Token ring, FDDI, X.25, ána až v koncových zařízeních (počítačích) a umožňuje proto přizpůsobit chování sítě potřebám aplikace. Poskytuje spojované (protokol TCP, spolehlivý) či nespojované (UDP, nespolehlivý) transportní služby.

Síťová vrstva

Vrstva zajišťuje především síťovou adresaci, směrování a předávání datagramů. Protokoly: IP, ARP, RARP, ICMP, IGMP, IGRP, IPSEC. Je implementována ve všech prvcích sítě - směrovačích i koncových zařízeních.

Transportní vrstva

Transportní vrstva je implementována až v koncových zařízeních (počítačích) a umožňuje proto přizpůsobit chování sítě potřebám aplikace. Poskytuje spojované (protokol TCP, spolehlivý) či nespojované (UDP, nespolehlivý) transportní služby.

Aplikační vrstva

Aplikační protokoly používají vždy jednu ze dvou základních služeb transportní vrstvy: TCP nebo UDP, případně obě dvě (např. DNS). Pro rozlišení aplikačních protokolů se používají tzv. porty, což jsou domluvená číselná označení aplikací. Každé síťové spojení aplikace je jednoznačně určeno číslem portu a transportním protokolem (a samozřejmě adresou počítače).

3.1 Základní protokoly

IP (anglicky *Internet Protocol*) je datový protokol používaný pro přenos dat přes paketové sítě. Tvoří základní protokol dnešního Internetu.

Data se v IP síti posílají po blocích nazývaných datagramy. Jednotlivé datagramy putují sítí zcela nezávisle, na začátku komunikace není potřeba navazovat spojení či jinak „připravovat cestu“ datům, přestože spolu třeba příslušné stroje nikdy předtím nekomunikovaly.

IP v doručování datagramů poskytuje nespolehlivou službu, označuje se také jako *best effort* – „nejlepší úsilí“; tj. všechny stroje na trase se datagram snaží podle svých možností poslat blíže k cíli, ale nezaručují prakticky nic. Datagram vůbec nemusí dorazit, může být naopak doručen několikrát a neručí se ani za pořadí doručených paketů. Pokud aplikace potřebuje spolehlivost, je potřeba ji implementovat v jiné vrstvě síťové architektury, typicky protokoly bezprostředně nad IP.

Pokud by síť často ztrácela pakety, měnila jejich pořadí nebo je poškozovala, výkon sítě pozorovaný uživatelem by byl malý. Na druhou stranu příležitostná chyba nemívá pozorovatelný efekt. Navíc se obvykle používá vyšší vrstva, která ji automaticky opraví.

Každé síťové rozhraní komunikující prostřednictvím IP má přiřazeno jednoznačný identifikátor, tzv. IP adresu. V každém datagramu je pak uvedena IP adresa odesilatele i příjemce. Na základě IP adresy příjemce pak každý počítač na trase provádí rozhodnutí, jakým směrem paket odeslat, tzv. směrování (*routing*); na starosti to mají hlavně specializované stroje označované jako směrovače (routery).

Dnes se nejčastěji používá verze označovaná číslem 4, nazývaná IPv4. IPv6 je navrhovaný a chystaný nástupce IPv4. Internetu pozvolna docházejí adresy (přesněji nebýt NATu a organizačních opatřeních zpřísňujících přidělování adres, zavedených v polovině 90. let, už by došly), a IPv6 má kromě jiného adresy 128bitové, které poskytují větší adresní prostor než 32bitové adresy v IPv4 (IPv4 má miliardy adres, IPv6 stovky sextiliónů).

Verze 0 až 3 jsou buď rezervované nebo nepoužité. Verze 5 (IPv5) byla použita pro experimentální proudový protokol (*stream protocol*). Některá další čísla verzí byla přiřazena pro experimentální protokoly, které se v praxi neobjevují. Nejnovější verze IPv6 nahradí stávající vzhledem k faktu, že adresy IPv4 i přes provedená úsporná opatření díky rozvoji internetu stále ubývají a mezi lety 2010 až 2011 by se mohly všechny vyčerpat. Nový protokol bude klást určité nároky směrem na vybavenost osobních počítačů i jiných zařízení. Moderní operační systémy (Windows XP, Windows Vista, Mac OS X, Linux) jsou již na implementaci připravené, ale je nutné upravit i všechny síťové aplikace.[2]

ARP (Address Resolution Protocol) se používá k nalezení fyzické adresy MAC podle známé IP adresy. Protokol v případě potřeby vyšle datagram s informací o hledané IP adrese a adresuje ho všem stanicím v síti. Uzel s hledanou adresou reaguje odpovědí s vyplněnou svou MAC adresou. Pokud hledaný uzel není ve stejném segmentu, odpoví svou adresou příslušný směrovač.

Příbuzný protokol RARP (Reverse Address resolution Protocol) má za úkol najít IP adresu na základě fyzické adresy.

ICMP (Internet Control Message Protocol) slouží k přenosu řídících hlášení, které se týkají chybových stavů a zvláštních okolností při přenosu. Používá se např. v programu ping pro testování dostupnosti počítače, nebo programem *traceroute* pro sledování cesty paketů k jinému uzlu.

TCP (Transmission Control Protocol) vytváří virtuální okruh mezi koncovými aplikacemi, tedy spolehlivý přenos dat.

Vlastnosti protokolu:

– spolehlivá transportní služba, doručí adresátovi všechna data bez ztráty a ve správném pořadí

– služba se spojením, má fáze navázání spojení, přenos dat a ukončení spojení

– transparentní přenos libovolných dat

– plně duplexní spojení, současný obousměrný přenos dat

– rozlišování aplikací pomocí portů

UDP (User Datagram Protocol) poskytuje nespolehlivou transportní službu pro takové aplikace, které nepotřebují spolehlivost, jakou má protokol TCP. Nemá fázi navazování a ukončení spojení a už první segment UDP obsahuje aplikační data. UDP je používán aplikacemi jako je DHCP, TFTP, SNMP, DNS a BOOTP.

Protokol používá podobně jako TCP čísla portů pro identifikaci aplikačních protokolů.

3.2 Další protokoly:

Aplikační protokoly (služby):

DNS – systém doménových jmen
DHCP – dynamické přidělování IP adres
FTP – přenos souborů po síti
TFTP – jednoduchý protokol pro přenos souborů
HTTP – přenos hypertextových dokumentů (WWW)
WEBDAV – rozšíření HTTP o práci se soubory
IMAP – umožňuje manipulovat s jednotlivými e-mail zprávami na poštovním serveru
IRC – jednoduchý chat po internetu
NNTP – umožňuje číst a umísťovat do sítě zprávy typu news
NFS – síťový systém souborů, který umožňuje transparentní sdílení vzdálených souborů jakoby byly lokální
NTLM – autentizační protokol Windows
NTP – synchronizace času (šíření přesného času)
POP3 – protokol pro získání pošty z poštovního serveru
SMB - sdílení souborů a tiskáren v sítích Windows
SMTP – zasílání elektronické pošty
SNMP – je určen pro správu síťových uzlů
Telnet – protokol virtuálního terminálu
SSH – bezpečný shell
X11 – zobrazování oken grafických programů v Unixech
XMPP – rozšiřitelný protokol pro zasílání zpráv a sledování přítomnosti (protokol Jabber)

4 Návrh pracoviště pro ověření bezpečného přihlášení

Pracoviště pro bezpečné přihlášení do sítě je tvořeno:

– PC s operačním systémem Linux (Ubuntu 8.10.) a USB 2.0 portem

– Čtečkou otisku prstů Eikon

– Softwarem pro komunikaci mezi PC a čtečkou

PC s operačním systémem Linux (Ubuntu 8.10.) a USB 2.0 portem

Zadání diplomové práce specifikovalo řešit problém pod systémem Linux, proto bylo nutné nainstalovat do PC se systémem Windows i systém Linux. Pro moji úlohu jsem si zvolil Linux verze Ubuntu.8.10. PC musí dále obsahovat USB 2.0, aby mohlo dojít k propojení mezi čtečkou a PC.

Čtečka otisku prstů

Existuje nepřeberné množství typů čteček otisku prstů a jejich případné použití v různých aplikacích. Nejprve jsem pracoval s vývojovým kitem SFM3500 EVK. Ale po seznámení se s jeho funkcí jsem zjistil, že nepracuje pod systémem Linux, což je hlavní požadavek mé diplomové práce. Proto jsem si vybral čtečku Eikon od firmy UPEK, která je plně podporována operačním systémem Linux, lze se přihlašovat jak do sítě tak i do systému.

Software pro komunikaci mezi PC a čtečkou

Pro komunikaci mezi PC a čtečkou karet a pro jednotlivé snímání vzorků otisku prstů je použit software lnxdemo

4.1 Čtečka otisku prstů Eikon

Jak jsem se již zmínil, tak pro moji praktickou část jsem si zvolil čtečku otisku prstů Eikon od firmy UPEK, která je zobrazena na Obr.20.

Obr.20. Čtečka otisku prstů Eikon

Vlastnosti čtečky Eikon:

Senzor	UPEK swipe sensor TouchStrip® TCS4C
Technologie senzoru	Kapacitní CMOS senzor
Komunikační rozhraní	USB 2.0
Snímací rychlost	Větší než 39 cm/s
Rozměry senzoru	14 x 4,5 mm
Aktivní snímací plocha	9,6 x 0,2 mm
Rozlišení otisku	192 x512 pixelů
Pixelový rastr	50μm
Rozlišení	508 dpi
Certifikáty	CE, UL, FCC, USB 2.0, WHQL

Tato čtečka používá pro snímání vzorku tzv. šablonování. Jak již bylo vysvětleno jde o techniku kdy se biometrický vzorek získává přejížděním prstem po senzoru.

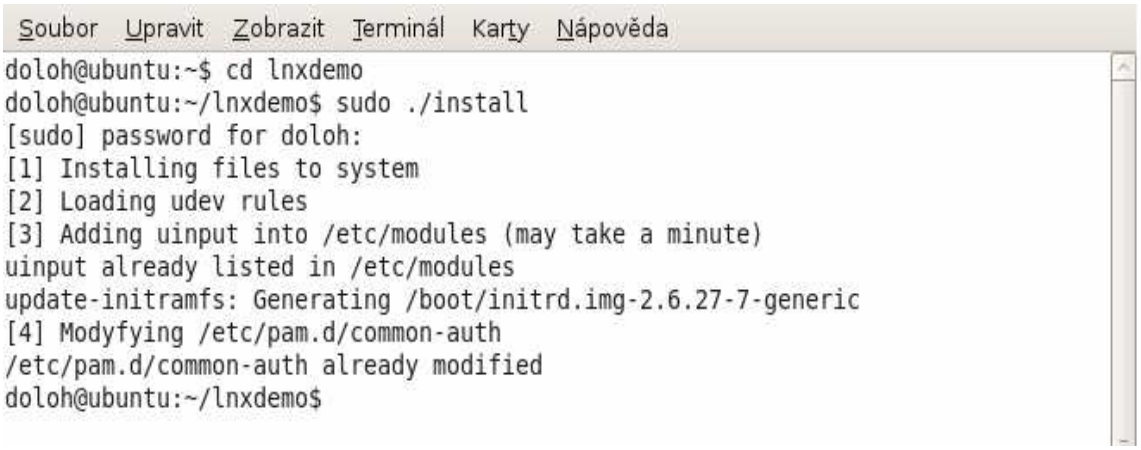
Výhodou šablonovaného snímání je, že snímač zůstává stále čistý, jelikož každý sejmutý pruh vyčistí senzor; na snímači nezůstávají skryté (latentní) staré otisky; uživatel nemá pocit ‚zanechaného' otisku prstu a snímání je rychlé.

4.2 Instalace softwaru čtečky Eikon

Pro komunikaci mezi PC a čtečkou Eikon je použita softwarová aplikace lnxdemo. Tato aplikace je vyvíjena přímo společností Upek a není určená pro komerční účely. Aplikace podporuje nejen přihlášení do sítě, ale i do systému. Pro moji práci jsem prováděl nastavení aplikace pro bezpečné přihlašování do sítě.

Průběh instalace:

– nejdříve zkopírujeme SW do	*/home/doloh/`lnxdemo.tar.gz`*
– otevření terminálu	*Aplikace > Příslušenství > Terminál*
– rozbalení SW příkazem	*$ tar xfvz lnxdemo.tar.gz*
– takto jsme získali složku lnxdemo	*/home/doloh/lnxdemo*
– instalace SW v terminálu	*cd lnxdemo*
–	*sudo ./install*



Obr.21. Postup instalace softwaru Fingerprint Enrollment

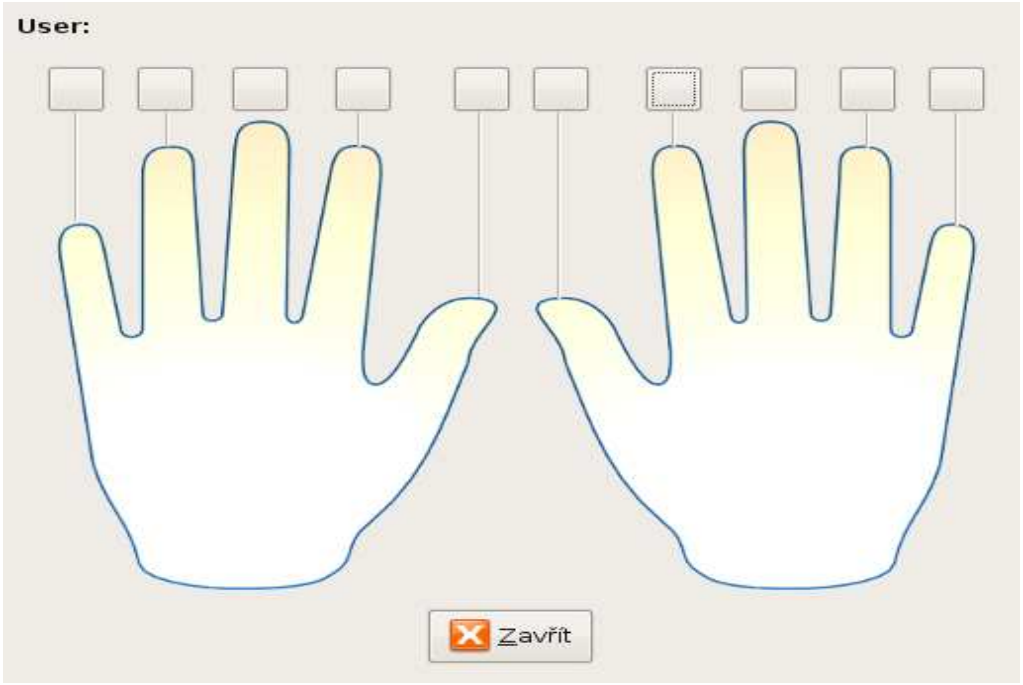
Jestliže proběhne instalace bez problému, tak je nám k dispozici grafické rozhraní aplikace Fingerprint Enrollment, které najdeme v *Systém >Správa > Fingerprint Enrollment.*

Instalace tohoto softwaru nainstaluje PAM modul *pam_upek.so*, který je potřebný pro přihlašování do sítě pomocí čtečky.

PAM (Pluggable Authentication Modules**)** je mechanizmus pro integraci více nízko-úrovňových autentizačních schémat do API, což umožňuje programům pracujícím s autentizací, uložit uživatelské údaje nezávisle na použitém mechanizmu přihlášení. PAM byl poprvé vyvinut v roce 1996 firmou Sun Microsystems, později se stal standardním modulem UNIX/Linux systémů.

4.3 Nastavení aplikace Fingerprint Enrollment

Aplikace Fingerprint Enrollment slouží pro snímání vzorků otisku prstů, jde o jednoduchou a přehlednou grafickou aplikaci. Otevřeme ji *Systém >Správa > Fingerprint Enrollment.* Okno aplikace Fingerprint Enrollment vidíme na obr.22.



Obr.22.Aplikace Fingerprint Enrollment

Na Obr.22 vidíme, že aplikace podporuje nasnímání kteréhokoli prstu, já jsem si zvolil ukazováček pravé ruky.

Postup snímání je následující

– připojíme čtečku Eikon do PC přes USB 2.0 port

– rozsvítí se kontrolní dioda na čtečce signalizující, že čtečka je připravena ke snímání

– přiložíme zvolený prst ke čtečce a přejíždíme po senzoru definovaným směrem

– dochází ke snímání otisku prstu tzv.šablonováním

– je třeba nasnímat otisk několikrát, aby došlo ke shromáždění většího počtu biometrických dat potřebných k pozdějšímu porovnávání s daným vzorkem

– v mém případě je třeba nasnímat otisk devětkrát, tyto vzorky se ukládají do upekX.bir

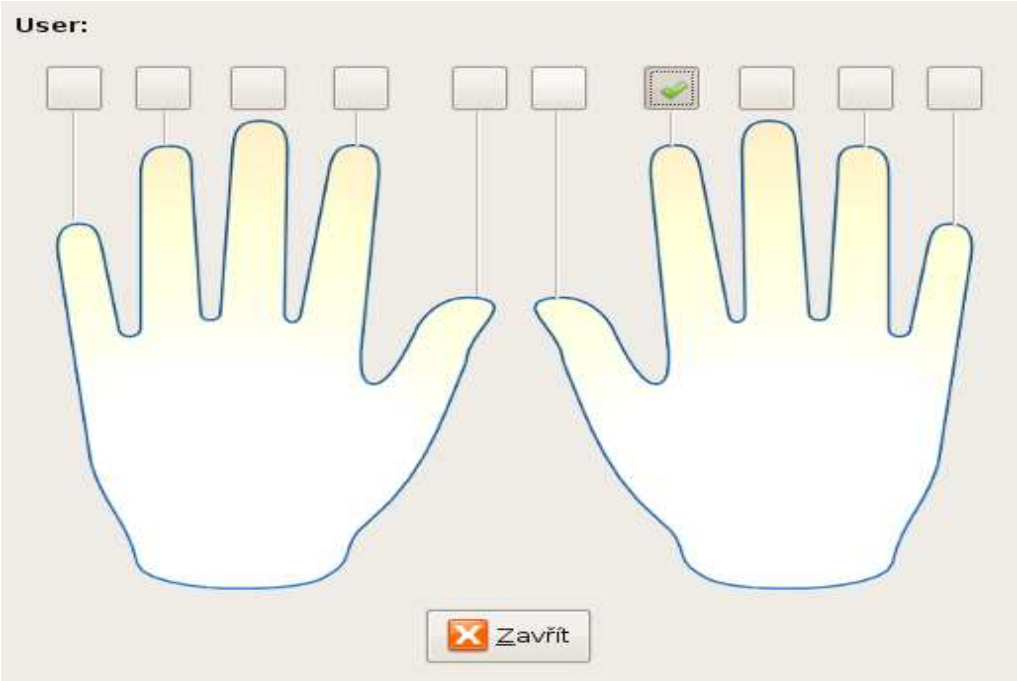
– po dokončení snímání je potřeba nainstalovat aplikaci adobe flash player, která je potřebná pro bezpečné přihlášení do sítě

Obr.23. Snímání otisku prstu

Obr.24. Dokončení snímání otisku prstu

4.4 Postup přihlášení do sítě

Jestliže jsme úspěšně nasnímali potřebný počet biometrických dat , jak vidíme na Obr.25., můžeme přistoupit k vlastnímu přihlášení do sítě.



Obr.25. Dokončení nasnímání dostatečného počtu biometrických dat

Pro mé zadání bezpečného přihlášení do sítě jsem si zvolil přihlášení na email seznam.cz.

Postup přihlášení je následující:

– spustil jsem internet pomocí prohlížeče Mozilla Firefox

– přešel jsem na stránky seznam.cz *http://seznam.cz*

– přihlásil jsem se k emailu pomocí přihlašovacího jména a hesla viz. Obr.26

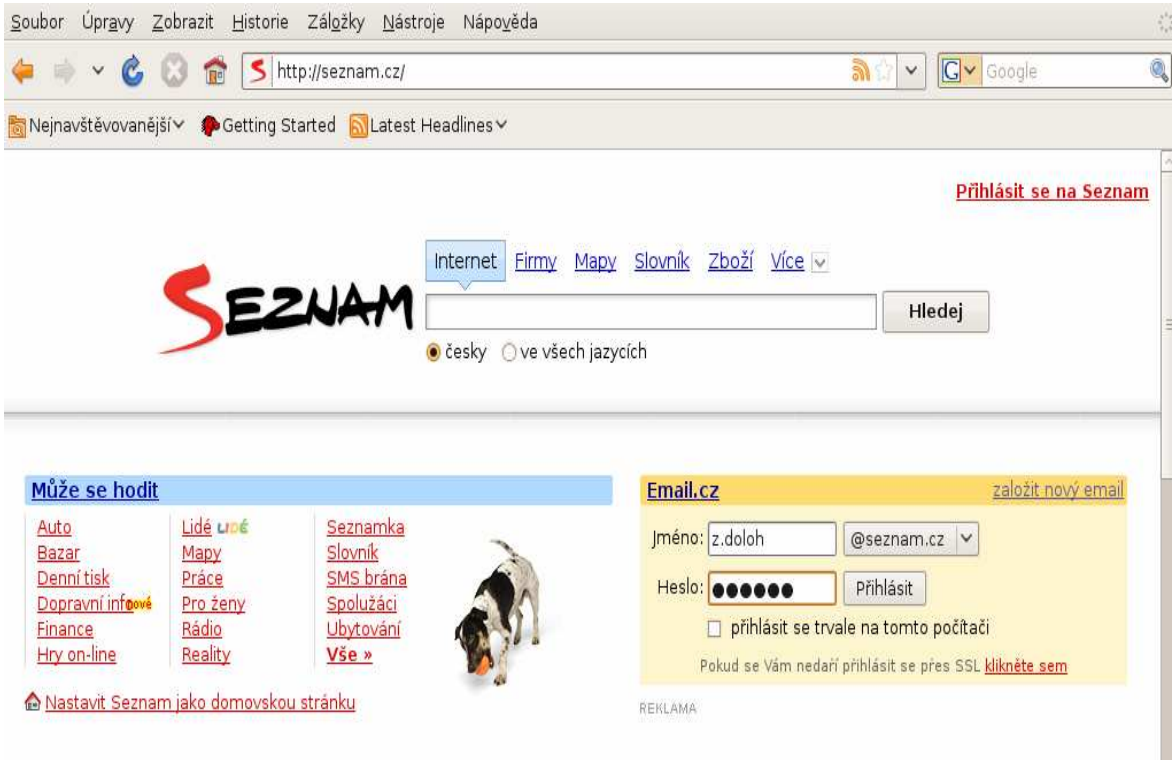
– poté co jsem se přihlásil k emailu jsem zadal volbu *Zapamatovat uživatele* viz.Obr.27

– odhlásil jsem se z emailu

– po opětovném přihlášení na email vyskočilo grafické okno (Obr.28.) s volbou přihlášení k emailu pomocí otisku prstu

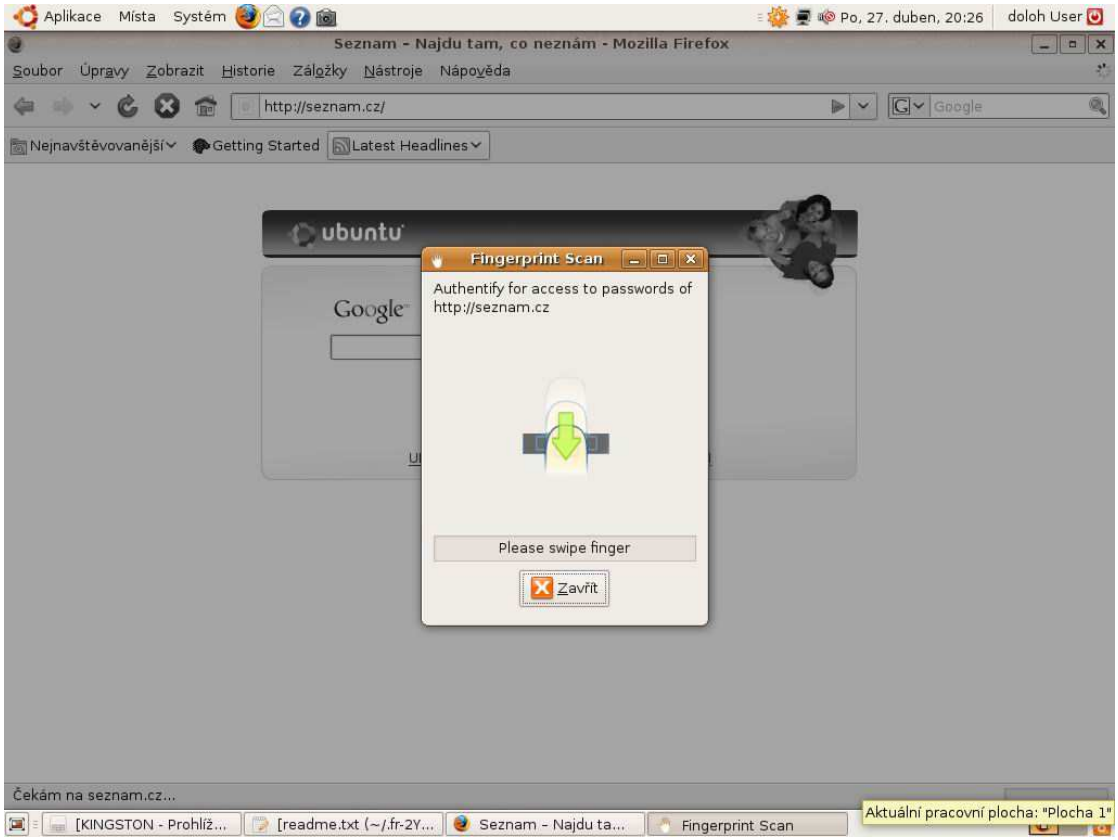
– přiložil jsem ukazováček pravé ruky ke snímači a přejel jsem definovaným směrem, jestliže došlo ke shodě s uloženým vzorkem v databázi, tak došlo k potvrzení shody a připojení k emailu pomocí uloženého hesla (Obr.30)

– jestliže nedojde ke shodě, nebo uživatel se nechce přihlásit k emailu, tak dochází pouze na přesměrování na stránky seznam.cz.(Obr.31)

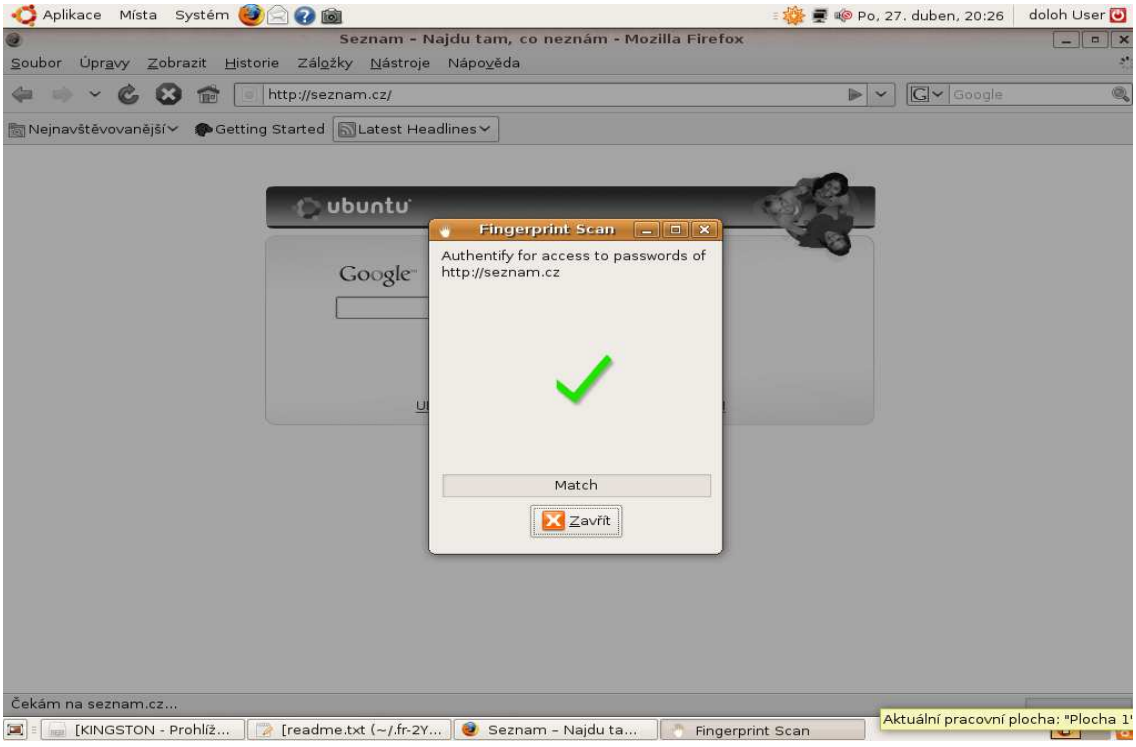


Obr.26. Přihlášení k emailu

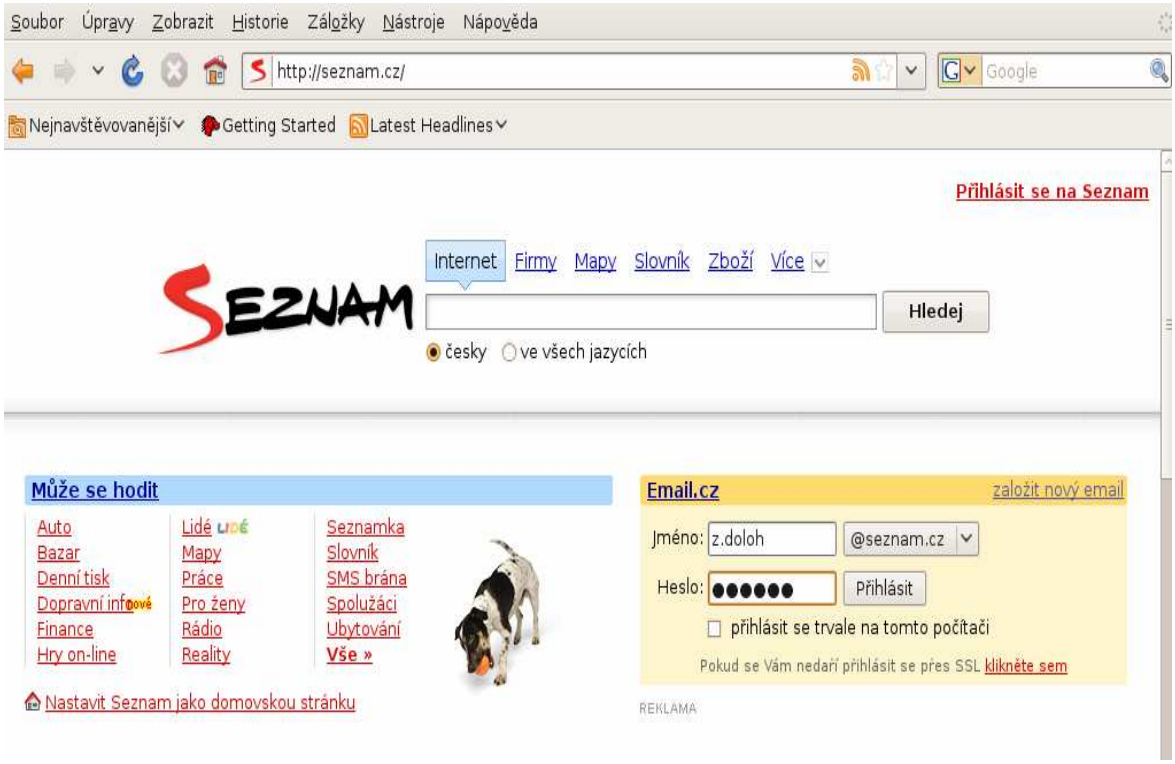
Obr.27. Zapamatování přihlašovacího hesla



Obr.28.Přihlášení k emailu pomocí otisku prstu

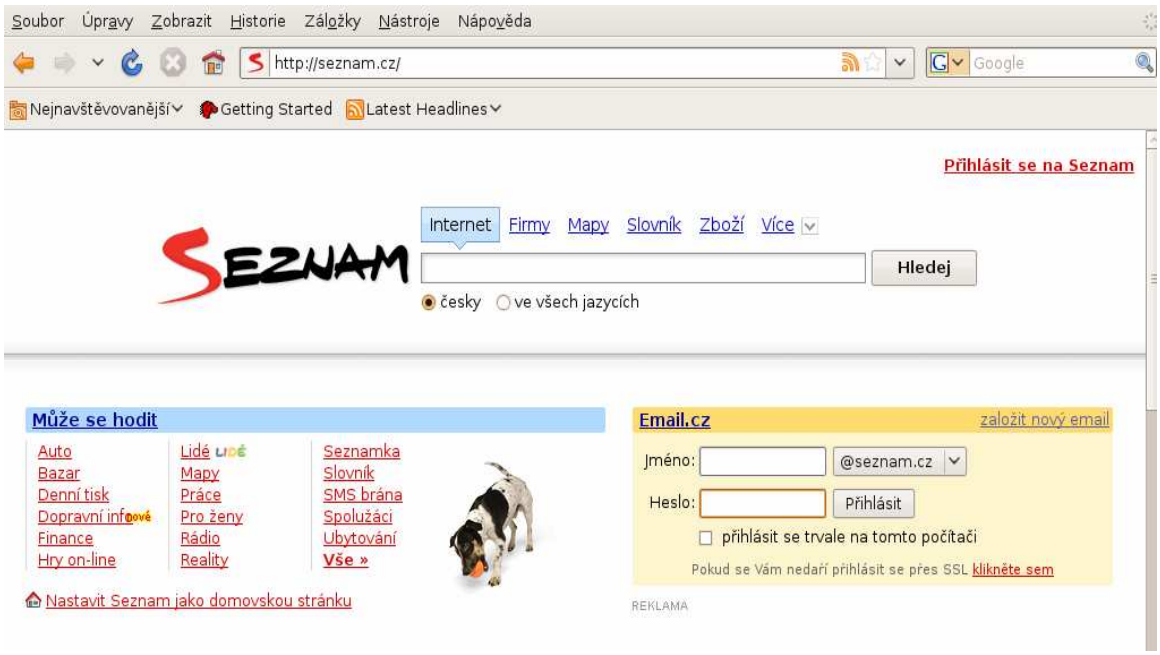


Obr.29. Potvrzení shody snímaného vzorku s nasnímanými vzorky



Obr.30. Úspěšné přihlášení k emailu pomocí otisku prstu

Jestliže vzorek otisku není shodný tak se dostaneme pouze na domovskou stránku seznam.cz bez přihlášení k emailu viz. Obr.31.



Obr.31. Neúspěšné přihlášení k emailu

5 Grafická prezentace problematiky pomocí Flashe

Jako poslední bod diplomové práce jsem měl udělat grafickou prezentaci problematiky biometrie.

Tato prezentace se skládá z následujících bodů:

– vysvětlení pojmu biometrie

– vlastnosti biometrické metody otisku prstů

– různé technologie snímání otisku prstů

– popis čtečky otisku prstů Eikon

– průběh celé instalace softwaru pro bezpečné přihlašování lnxdemo

– nastavení softwaru Fingerprint Enrollment

– postup snímání jednotlivých vzorků pomocí aplikace Fingerprint Enrollment

– postup přihlášení do sítě k emailu na stránce seznam.cz

– zhodnocení technologie

Prezentace byla vytvořena v programu PowerPoint 2003 a s pomocí programu iSpring Presenter byla překonvertována do Flashe. Program iSpring Presenter je uložen na CD, které je součástí diplomové práce. Grafická prezentace je uvedena na CD přiloženém v diplomové práci.

Obr.31 Úvodní snímek grafické prezentace

6 Závěr

Biometrické metody jsou velmi rychle se rozvíjející metody pro bezpečné přihlašování, jak do sítě, tak do systému. Jsou velice bezpečné , využívají faktu, že každý člověk má své jedinečné fyziologické vlastnosti. Mezi nejčastěji používanou biometrickou metodu řadíme právě otisk prstu, jehož biometrický vzorek je univerzální, jedinečný a stálý.

V mé diplomové práci jsem měl zprovoznit přihlašování do sítě pod systémem Linux, pod kterým jen zřídka pracují čtečky otisku prstů, což je škoda, jelikož v poslední době se zvyšuje obliba práce pod operačním systémem Linux. Po dlouhém hledání jsem si zvolil čtečku Eikon od firmy Upek, která jako jedna z mála pracuje pod systémem Linux. Ke komunikace mezi PC a čtečkou Eikon je zapotřebí nainstalovat program lnxdemo. Aplikace lnxdemo pro přihlašování do sítě je od firmy Upek, je to pouze demo (prototyp), které není použito pro komerční účely. Toto demo mně bylo poskytnuto k dalším úpravám, které byly potřebné k zprovoznění služby přihlášení do sítě. Aplikace pracovala nejen pod systémem Ubuntu 8.10, ale i pod Debianem a live distribucí Ubuntu 8.10. Pro přihlašování do sítě bylo potřeba nainstalovat k aplikaci lnxdemo program adobe flash player, který byl zapotřebí k tomu, aby se objevila nabídka výzvy nasnímání otisku prstů při přihlášení k emailu, poněvadž jde o flashovou aplikaci.

Čtečka Eikon využívá pro svoji činnost kapacitní CMOS senzor a způsob snímání tzv. šablonování.

V diplomové práci jsem se zprvu zabýval i vývojovým kitem SFM3500 EVK, který je od firmy Suprema, ale hned zpočátku se ukázalo, že tento vývojový kit není vhodný pro pracovní prostředí Linux.

Přihlášení pomocí otisku prstů do sítě je velmi pohodlné a jednoduché. Při instalaci softwaru i nastavování softwaru nedošlo k žádným zásadním problémům, jediný problém spočívá v tom, že při snímání otisku prstů musí člověk dbát na správný pohyb prstu při snímaní otisku senzorem. Několikrát se mi stalo, že došlo k chybnému vyhodnocení mého vzorku vlivem špatného pohybu prstu přes snímač.

Tato práce je přínosná jako návod pro bezpečné přihlášení do sítě pod systémem Linux, je zde uveden přesný postup instalace a nastavení jak čtečky, tak i samostatného softwaru.

7 Seznam použité literatury

[1] RAK, R a kolektiv, et al. *Biometrie a identita člověka ve forezních a komerečních aplikacích*. 1. vyd. Praha : Grada Publishing, a.s., 2008. 664 s.

[2] DOSTÁLEK, L. a kolektiv, et al. *Velký průvodce protokoly TCP/IP:Bezpečnost.* Brno: Computers press, 2003. 572 s. ISBN 80-7226-849-X

[3] Biometrie [online,]Dostupný z WWW:
http://cs.wikipedia.org/wiki/Biometrie

[4] Biometrie: kontroverzní technologie[online] 2006 [citováno 2006-03-01],
Dostupný z WWW:
http://www.symantec.com/cs/cz/norton/library/article.jsp?aid=article2_03_06

[5] CHURÝ, Lukáš, *Cestovní doklady s biometrickými prvky* [online] 2006 [2006-04-21]
Dostupný z WWW:
http://programujte.com/index.php?akce=clanek&cl=2006041805-cestovni-doklady-s-biometrickymi-prvky-cdbp-

[6] KLEN, Petr, Ph.D., *AppTima s. r. o.*, [online], 2003, [2003-11-01]
Dostupný z WWW:
http://www.odbornecasopisy.cz/index.php?id_document=28978

[7] COUFAL, Tomáš. *Finger Chip*, [online], 2007, [2007-0829]
Dostupný z WWW:
http://hw.cz/teorie-praxe/art2020-co-je-fingerchip.html

[8] Biometrika:Snímače otisku prstu, [online], 2005, [2005-10-16]
Dostupný z WWW:
http://www.specialista.info/view.php?nazevclanku=biometrika-snimace-pro-otisk-prstu&cisloclanku=2005100402

[9] OCHODKOVÁ, Eliška. *Kryptografie a počítačová bezpečnost 2006* [online],2006
Dostupný z WWW: http://wiki.cs.vsb.cz/images/a/a9/Kb07.pdf

8 Seznam příloh na CD

Příloha I	Grafická prezentace problematiky biometrie ve Flash
Příloha II	Podklady pro Flash prezentaci
Příloha III	Studijní materiály
Příloha IV	Srovnání různých biometrických technologií
Příloha V	Software pro čtečku Eikon